IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO. 074273/0163

Applicant: Satoshi OBANA

Title: ENCRYPTION AND DECRYPTION WITH ENDURANCE TO CRYPTANALYSIS METHOD

Appl. No.: Unassigned

Filing Date: 04/20/2000

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application No. 11-114230 filed April 21, 1999.

Respectfully submitted,

April 20, 2000
Date

for Phillip J. Articola
David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

Reg. No. 38,819

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

OBANA
074273/0163

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ４月２１日

出 願 番 号
Application Number: 平成１１年特許願第１１４２３０号

出 願 人
Applicant (s): 日本電気株式会社

２０００年 ２月１８日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３００７６３４

【書類名】　特許願
【整理番号】　33509445
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　尾花　賢
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100088890
　【弁理士】
　【氏名又は名称】　河原　純一
【手数料の表示】
　【予納台帳番号】　009690
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9001717
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化装置，復号装置，および暗号化・復号装置

【特許請求の範囲】

【請求項１】　乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、

平文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、

前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化装置。

【請求項２】　乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、

平文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、

前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に

対する条件分岐決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化装置。

【請求項３】　乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、

平文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、

前記暗号化演算手段による暗号化処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化装置。

【請求項４】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段，平文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段，および前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段として機能させるための暗号化処理プログラムを記録した記録媒体。

【請求項５】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続き

を選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段，平文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段，および前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段として機能させるための暗号化処理プログラムを記録した記録媒体。

【請求項６】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段，平文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段，および前記暗号化演算手段による暗号化処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段として機能させるための暗号化処理プログラムを記録した記録媒体。

【請求項７】　出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかである乱数生成装置を備えたことを特徴とする請求項１，請求項２，または請求項３記載の暗号化装置。

【請求項８】　出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかである乱数生成装置の機能を有する暗号化処理プログラムを記録したことを特徴とする請求項４，請求項５，または請求項６記載の記録媒体。

【請求項９】　乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、

暗号文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、

前記復号演算手段による復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段と

を備えたことを特徴とする復号装置。

【請求項１０】　乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、

暗号文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、

前記復号演算手段による復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする復号装置。

【請求項１１】　乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、復号処理中に意図的に挿

入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、

暗号文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、

前記復号演算手段による復号処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする復号装置。

【請求項１２】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段，暗号文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段，および前記復号演算手段による復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段として機能させるための復号処理プログラムを記録した記録媒体。

【請求項１３】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段，暗号文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させ

つつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段，および前記復号演算手段による復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段として機能させるための復号処理プログラムを記録した記録媒体。

【請求項１４】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段，暗号文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段，および前記復号演算手段による復号処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段として機能させるための復号処理プログラムを記録した記録媒体。

【請求項１５】　出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置を備えたことを特徴とする請求項９，請求項１０，または請求項１１記載の復号装置。

【請求項１６】　出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置の機能を有する復号処理プログラムを記録したことを特徴とする請求項１２，請求項１３，または請求項１４記載の記録媒体。

【請求項１７】　乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中および復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、

処理データおよび処理内容を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、

前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化・復号装置。

【請求項１８】　乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きおよび復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化・復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、

処理データおよび処理内容を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、

前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化・復号装置。

【請求項１９】　乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理および復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、

処理データおよび処理内容を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、

前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化・復号装置。

【請求項２０】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中および復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段，処理データおよび処理内容を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段，ならびに前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存中間データ変更操作を適

用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段として機能させるための暗号化・復号処理プログラムを記録した記録媒体。

【請求項２１】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きおよび復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化・復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段，処理データおよび処理内容を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段，ならびに前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段として機能させるための暗号化・復号処理プログラムを記録した記録媒体。

【請求項２２】　コンピュータシステムを、乱数を出力する乱数生成装置，前記乱数生成装置から出力される乱数を入力として、暗号化処理および復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段，処理データおよび処理内容を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数

生成装置の出力に依存しない平文を出力する暗号化・復号演算手段，ならびに前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段として機能させるための暗号化・復号処理プログラムを記録した記録媒体。

【請求項２３】　暗号化処理の際に出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかであり、復号処理の際に出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置を備えたことを特徴とする請求項１７，請求項１８，または請求項１９記載の暗号化・復号装置。

【請求項２４】　暗号化処理の際に出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかであり、復号処理の際に出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置の機能を有する暗号化・復号処理プログラムを記録したことを特徴とする請求項２０，請求項２１，または請求項２２記載の記録媒体。

【請求項２５】　平文に加えて暗号化鍵を入力とする暗号化演算手段を備えることを特徴とする請求項１，請求項２，請求項３，または請求項７記載の暗号化装置。

【請求項２６】　平文に加えて暗号化鍵を入力とする暗号化演算手段の機能を有する暗号化処理プログラムを記録したことを特徴とする請求項４，請求項５，請求項６，または請求項８記載の記録媒体。

【請求項２７】　暗号文に加えて復号鍵を入力とする復号演算手段を備えることを特徴とする請求項９，請求項１０，請求項１１，または請求項１５記載の復号装置。

【請求項２８】　暗号文に加えて復号鍵を入力とする復号演算手段の機能を有する復号処理プログラムを記録したことを特徴とする請求項１２，請求項１３，請求項１４，または請求項１６記載の記録媒体。

【請求項２９】　暗号化処理の際に処理データに加えて暗号化鍵を入力とし復号処理の際に処理データに加えて復号鍵を入力とする暗号化・復号演算手段を備

えることを特徴とする請求項１７，請求項１８，請求項１９，または請求項２３記載の暗号化・復号装置。

【請求項３０】　暗号化処理の際に処理データに加えて暗号化鍵を入力とし復号処理の際に処理データに加えて復号鍵を入力とする暗号化・復号演算手段の機能を有する暗号化・復号処理プログラムを記録したことを特徴とする請求項２０，請求項２１，請求項２２，または請求項２４記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号化鍵を用いて平文の暗号化を行い暗号文を生成する暗号化装置および復号鍵を用いて暗号文の復号を行い平文を生成する復号装置ならびに暗号化装置と復号装置との機能を併有する暗号化・復号装置に関する。なお、暗号化装置と復号装置とは、それぞれの入力は異なるが構成や演算の内容は同様であるので、以下では主に暗号化装置で代表させて説明を行う。

【０００２】

【従来の技術】

従来の暗号化装置は、入力装置と記憶装置と暗号化処理装置と出力装置とから構成されており、次のように動作する。

【０００３】

すなわち、入力装置より暗号化処理装置に平文が入力され、平文を入力した暗号化処理装置は暗号化処理の中間段階で必要となる中間データを記憶装置に格納しつつ、常に予め定められた一定の処理順序に従って暗号化処理を行い、生成した暗号文を出力装置を通じて出力する。このとき、暗号化処理の開始時から特定の暗号化中間処理手続きが開始されるまでに要する時間は、おおよそ一定になる。

【０００４】

なお、暗号アルゴリズムの実装方法については、『「Ａｐｐｌｉｅｄ　Ｃｒｙｐｔｏｇｒａｐｈｙ」（Ｂｒｕｃｅ　Ｓｈｎｅｉｅｒ著）　Ｊｏｈｎ　Ｗｉｅｌｅｙ　＆　Ｓｏｎｓ，Ｉｎｃ.，１９９６，ＩＳＢＮ　０－４７１－１１７０９

－９，ｐｐ．６２３－６７３』に詳しく述べられている。

【０００５】

【発明が解決しようとする課題】

上述した従来の技術による暗号化装置には、電力解析（シンプル・パワー・アナリシス）や電力差分解析（ディファレンシャル・パワー・アナリシス）と呼ばれる暗号解析法が有効であるという問題が存在する。

【０００６】

電力解析および電力差分解析は、現在のメモリやレジスタ等の半導体デバイスにおいて、特定の時刻に当該半導体デバイスの保持する値に変化があった場合に、当該時刻における消費電力が保持する値に変化がなかった場合と比較して大きくなるという特徴を利用して、暗号化装置が平文の暗号化を行っている複数の時点で暗号化装置が消費する電力を測定することにより、暗号化装置が保持している秘密鍵（暗号化鍵）等の秘密情報を特定する暗号解析法である。

【０００７】

電力解析や電力差分解析が有効に機能する条件としては、第１に消費電力を測定している各時点で行われている暗号化処理手続きが特定できること、第２に各時刻で測定した消費電力の値が当該時刻において暗号化装置内で行われている暗号化処理の演算結果を顕著に反映していること、の２点が挙げられる。

【０００８】

従来の暗号化装置（復号装置および暗号化・復号装置も同様）においては、上記の２点の条件が満たされてしまうために、先に述べたように、電力解析や電力差分解析が有効に機能し、暗号の解読が可能になりうるという問題点が存在した。

【０００９】

本発明の目的は、上述の点に鑑み、暗号化処理（復号処理も同様）の処理過程において乱数依存の状態変化を起こすことにより、消費電力を測定している各時点で行われている暗号化処理手続きを特定することを困難にすることで、電力解析および電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置（同様な復号装置および暗号化・復号装置を含む）を提供することにあ

る。

【００１０】

また、本発明の他の目的は、暗号化処理（復号処理も同様）の処理過程において乱数依存の状態変化を起こすことにより、各時刻で測定した消費電力の値と当該時刻に暗号化装置内で行われている暗号化処理との関連性を少なくすることで、電力解析および電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置（同様な復号装置および暗号化・復号装置を含む）を提供することにある。

【００１１】

なお、本発明に対する従来技術に関する特許公報としては、特開平９－２３０７８６号公報および特開平８－５０４０６７号公報がある。

【００１２】

上述の特開平９－２３０７８６号公報に記載された技術（データの暗号化方法及び装置）は、差分解読や線形解読を防止するための技術であり、暗号化の中間結果（本願発明における中間データ）を乱数には依存させずに変化させ、暗号化鍵を乱数に依存して変化させるものである。

【００１３】

また、上述の特開平８－５０４０６７号公報に記載された技術（暗号化通信装置内の改善された機密性に関する方法および装置）は、電力遮断時等に、暗号化装置内の揮発性メモリに格納された鍵情報を能動的に消去し、電力供給再開時に同鍵情報をリロードするための技術である。

【００１４】

これらの技術や当該両技術を組み合わせた技術では、最終的に出力される暗号文を乱数に依存しないようにすることは非常に困難である。これに対して、本発明の暗号化装置は、乱数生成装置によって出力される乱数に依存しない暗号文を出力するという性質を持っている（乱数に依存するのは中間データのみで、最終的な出力である暗号文は乱数に依存しない）。この点で、本発明は、上記の公報に記載された従来技術とは明確に異なっている。

【００１５】

【課題を解決するための手段】

本発明の暗号化装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、平文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを有する。

【００１６】

また、本発明の暗号化装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、平文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【００１７】

さらに、本発明の暗号化装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理中に意図的に挿入する実行

遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、平文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、前記暗号化演算手段による暗号化処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【００１８】

本発明の復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、暗号文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、前記復号演算手段による復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを有する。

【００１９】

また、本発明の復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、暗号文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生

成装置の出力に依存しない平文を出力する復号演算手段と、前記復号演算手段による復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【００２０】

さらに、本発明の復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、暗号文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、前記復号演算手段による復号処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【００２１】

本発明の暗号化・復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中および復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、処理データおよび処理内容を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段

階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを有する。

【００２２】

また、本発明の暗号化・復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きおよび復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化・復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、処理データおよび処理内容を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【００２３】

さらに、本発明の暗号化・復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理および復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、処理データおよび処理内容を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数

生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【００２４】

【発明の実施の形態】

次に、本発明について図面を参照して詳細に説明する。

【００２５】

（１）　第１の実施の形態

図１は、本発明の第１の実施の形態に係る暗号化装置の構成を示すブロック図である。

【００２６】

本実施の形態に係る暗号化装置は、入力装置１１０と、暗号化処理装置１２０と、記憶装置１３０と、乱数生成装置１４０と、出力装置１５０とを含んで構成されている。

【００２７】

これらの装置は、それぞれ、概略次のように動作する。

【００２８】

入力装置１１０は、暗号化処理の対象となる平文を暗号化処理装置１２０に対して供給する。

【００２９】

暗号化処理装置１２０は、乱数生成装置１４０から出力される乱数と入力装置１１０より入力される平文とを入力として、当該平文を暗号化処理装置１２０内部に格納された鍵（暗号化鍵）で暗号化した暗号文を出力装置１５０から出力する。

【００３０】

ここで、暗号化処理装置１２０は、暗号化演算手段１２１と、乱数依存性決定手段１２２と、中間データ制御手段１２３とを備えている。

【００３１】

暗号化演算手段１２１は、入力装置１１０を通して供給される平文を入力とし、暗号化演算手段１２１に格納されている暗号化鍵を用いて当該平文の暗号化を行う。暗号化演算手段１２１は、「中間データ制御手段１２３による中間データ（中間データ記憶部１３１に格納されているデータ）の乱数に依存した変更」を受けて状態を変化させつつ暗号化処理（複数の処理段階によって形成される暗号化処理）を実行し、最終的に当該平文を暗号化した暗号文を出力する。なお、暗号化演算手段１２１は、暗号化処理実行中の複数の時点で、暗号化演算手段１２１による暗号化処理の現在の処理段階を乱数依存性決定手段１２２に送る（これにより、適切な処理段階で乱数に依存した状態の変化を生じさせることができる）。

【００３２】

乱数依存性決定手段１２２は、暗号化演算手段１２１が出力する暗号化演算手段１２１の現在の処理段階を入力として、当該処理段階に基づいて中間データ制御手段１２３に中間データ変更要求を出力すべきか否かを判断し、「中間データ変更要求の出力」を決定した場合（現在の処理段階が乱数に依存した操作を適用すべき処理段階であると判断した場合）には中間データ制御手段１２３に中間データ変更要求を出力する。

【００３３】

中間データ制御手段１２３は、乱数依存性決定手段１２２より出力される中間データ変更要求を入力した場合に、乱数生成装置１４０に乱数要求信号を送ることによって乱数を取得し、取得した乱数に依存して中間データ記憶部１３１に格納された中間データを変化させる操作（乱数依存中間データ変更操作）を行う。

【００３４】

なお、中間データ制御手段１２３は、乱数依存中間データ変更操作を複数回適用することによって、乱数の効果を相殺するように構成されている。したがって、最終的に出力される暗号文は、乱数生成手段１４０から出力される乱数に依存しない。

【００３５】

記憶装置１３０は、中間データ記憶部１３１を備えている。

【００３６】

中間データ記憶部１３１は、暗号化処理装置１２０が行う暗号化処理中に保持する必要のある中間データを格納する。なお、上記に示す通り、乱数依存性決定手段１２２から中間データ制御手段１２３に中間データ変更要求があった場合には、中間データ記憶部１３１に格納されている中間データは中間データ制御手段１２３によって操作される。

【００３７】

乱数生成装置１４０は、暗号化処理装置１２０より乱数要求信号を受け取り、当該乱数要求信号に基づいて暗号化処理装置１２０に乱数を出力する。

【００３８】

図２は、本実施の形態に係る暗号化装置の処理を示す流れ図である。この処理は、平文入力ステップＡ１と、中間データ変更要求有無判定ステップＡ２と、乱数出力ステップＡ３と、乱数依存中間データ変更操作ステップＡ４と、暗号化処理一段階実行ステップＡ５と、暗号化処理終了判定ステップＡ６と、暗号文出力ステップＡ７とからなる。

【００３９】

次に、図１および図２を参照して、本実施の形態に係る暗号化装置の全体の動作について詳細に説明する。

【００４０】

まず、暗号化を行いたい平文が、入力装置１１０から暗号化処理装置１２０内の暗号化演算手段１２１に入力される（図２のステップＡ１）。

【００４１】

暗号化演算手段１２１は、暗号化演算手段１２１による暗号化処理の現在の処理段階を乱数依存性決定手段１２２に出力する。

【００４２】

乱数依存性決定手段１２２は、暗号化演算手段１２１より受け取った暗号化演算手段１２１の処理段階に関する情報を基に、現在の処理段階が中間データ記憶

部１３１に格納された中間データを乱数に依存して変更する処理段階であるか否かの判断を行い、「乱数に依存して中間データを変更する処理段階である」と判断した場合には中間データ制御手段１２３に中間データ変更要求を出力する。

【００４３】

中間データ制御手段１２３は、乱数依存性決定手段１２２からの中間データ変更要求があるか否かを判定する（ステップＡ２）。

【００４４】

中間データ制御手段１２３は、ステップＡ２で「中間データ変更要求がある」と判定した場合には、当該中間データ変更要求を受け取り、乱数要求（乱数要求信号）を乱数生成装置１４０に送り、当該乱数要求信号に基づいて乱数生成装置１４０から出力された乱数を得る（ステップＡ３）。

【００４５】

乱数を受け取った中間データ制御手段１２３は、記憶装置１３０内の中間データ記憶部１３１に格納されている中間データ（暗号化処理手段１２１が暗号化処理の中間段階において必要とするデータ）を受け取った乱数に依存して変更する乱数依存中間データ変更操作を行う（ステップＡ４）。

【００４６】

暗号化演算手段１２１は、ステップＡ４の乱数依存中間データ変更操作が終了した後に、またはステップＡ２で「中間データ変更要求がない」と判定した場合に、暗号化処理を一段階実行する（ステップＡ５）。

【００４７】

暗号化演算手段１２１は、暗号化処理を一段階実行したことで暗号化処理が終了したか否かを判定する（ステップＡ６）。

【００４８】

暗号化演算手段１２１は、ステップＡ６で「暗号化処理を一段階実行したことで暗号化処理が終了した」と判定した場合には、出力装置１５０に暗号文を出力し（ステップＡ７）、全体の処理を終了させる。

【００４９】

一方、暗号化演算手段１２１は、ステップＡ６で「暗号化処理が終了していな

い」と判定した場合（暗号化処理がまだ残されている場合）には、ステップＡ２に制御を戻して暗号化処理を継続させる。

【００５０】

次に、本実施の形態における効果について説明する。

【００５１】

本実施の形態では、暗号化処理の中間段階で必要なデータ（中間データ）が乱数に依存して変化しているために、中間データ間の演算を行っている時点の電力を測定することによって格納されている中間データの情報を引き出そうとしても、中間データの値が乱数による影響を受けているために消費電力の変化が生じているのか、実際の暗号化処理に必要なデータの影響によって消費電力の変化が生じているのかを判断することが困難になる。したがって、暗号化装置を電力解析や電力差分解析による暗号解析に対して耐性があるようにすることができる。

【００５２】

（２）　第２の実施の形態

図３は、本発明の第２の実施の形態に係る暗号化装置の構成を示すブロック図である。

【００５３】

図３を参照すると、本実施の形態に係る暗号化装置は、入力装置３１０と、暗号化処理装置３２０と、記憶装置３３０と、乱数生成装置３４０と、出力装置３５０とを含んで構成されている。

【００５４】

これらの装置は、それぞれ、概略次のように動作する。

【００５５】

入力装置３１０は、暗号化処理の対象となる平文を暗号化処理装置３２０に対して供給する。

【００５６】

暗号化処理装置３２０は、乱数生成装置３４０から出力される乱数と入力装置３１０より入力される平文とを入力として、当該平文を暗号化処理装置３２０の内部に格納された鍵（暗号化鍵）で暗号化した暗号文を出力装置３５０から出力

する。

【００５７】

ここで、暗号化処理装置３２０は、暗号化演算手段３２１と、乱数依存性決定手段３２２と、条件分岐制御手段３２３とを備えている。

【００５８】

暗号化演算手段３２１は、入力装置３１０を通して供給される平文を入力とし、暗号化演算手段３２１に格納されている暗号化鍵を用いて当該平文の暗号化を行う。暗号化演算手段３２１は、「条件分岐制御手段３２３による命令実行順序（暗号化処理手続きの実行順序）の決定および実行命令の選択（複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択すること）の乱数に依存した変更」を受けて状態を変化させつつ暗号化処理（複数の処理段階によって形成される暗号化処理）を実行し、最終的に当該平文を暗号化した暗号文を出力する。なお、暗号化演算手段３２１は、暗号化処理実行中の複数の時点で、暗号化演算手段３２１による暗号化処理の現在の処理段階を乱数依存性決定手段３２２に送る（これにより、適切な処理段階で乱数に依存した状態の変化を生じさせることができる）。

【００５９】

乱数依存性決定手段３２２は、暗号化演算手段３２１が出力する暗号化演算手段３２１の現在の処理段階を入力として、当該処理段階に基づいて条件分岐制御手段３２３に条件分岐決定要求を出力すべきか否かを判断し、「条件分岐決定要求の出力」を決定した場合（現在の処理段階が乱数に依存した操作を適用すべき処理段階であると判断した場合）には条件分岐制御手段３２４に条件分岐決定要求を出力する。

【００６０】

条件分岐制御手段３２３は、乱数依存性決定手段３２２より出力される条件分岐決定要求を入力した場合に、乱数生成装置３４０に乱数要求信号を送ることによって乱数を取得し、取得した乱数に依存して「実行順序を交換しても暗号化演算手段３２１の出力が変化しないような複数の暗号化処理手続きの実行順序の決定」および「どの処理手続きを実行しても暗号化演算手段３２１の出力が変化し

ないような複数の処理手続きの選択肢の中からの実行処理手続き（実際に実行する暗号化処理手続き）の選択」を行う操作（乱数依存条件分岐決定操作）を行う。

【００６１】

なお、条件分岐制御手段３２３は、前述のように暗号化演算手段３２１の出力が乱数に依存しないように乱数依存条件分岐決定操作を制御するように構成されている。したがって、最終的に出力される暗号文は、乱数生成手段３４０から出力される乱数に依存しない。

【００６２】

記憶装置３３０は、中間データ記憶部３３１を備えている。

【００６３】

中間データ記憶部３３１は、暗号化処理装置３２０が行う暗号化処理中に保持する必要のある中間データを格納する。

【００６４】

乱数生成装置３４０は、暗号化処理装置３２０より乱数要求信号を受け取り、当該乱数要求信号に基づいて暗号化処理装置３２０に乱数を出力する。

【００６５】

図４は、本実施の形態に係る暗号化装置の処理を示す流れ図である。この処理は、平文入力ステップＢ１と、条件分岐決定要求有無判定ステップＢ２と、乱数出力ステップＢ３と、乱数依存条件分岐決定操作ステップＢ４と、暗号化処理一段階実行ステップＢ５と、暗号化処理終了判定ステップＢ６と、暗号文出力ステップＢ７とからなる。

【００６６】

次に、図３および図４を参照して、本実施の形態に係る暗号化装置の全体の動作について詳細に説明する。

【００６７】

まず、暗号化を行いたい平文が、入力装置３１０から暗号化処理装置３２０内の暗号化演算手段３２１に入力される（図４のステップＢ１）。

【００６８】

暗号化演算手段３２１は、暗号化演算手段３２１における暗号化処理の現在の処理段階を乱数依存性決定手段３２２に出力する。

【００６９】

乱数依存性決定手段３２２は、暗号化演算手段３２１より受け取った暗号化演算手段３２１の処理段階に関する情報を基に、現在の処理段階が乱数に依存した条件分岐の決定を行う処理段階であるか否かの判断を行い、「乱数に依存した条件分岐の決定を行う処理段階である」と判断した場合には条件分岐制御手段３２３に条件分岐決定要求を出力する。

【００７０】

条件分岐制御手段３２３は、乱数依存性決定手段３２２からの条件分岐決定要求があるか否かを判定する（ステップＢ２）。

【００７１】

条件分岐制御手段３２３は、ステップＢ２で「条件分岐決定要求がある」と判定した場合には、当該条件分岐決定要求を受け取り、乱数要求（乱数要求信号）を乱数生成装置３４０に送り、当該乱数要求信号に基づいて乱数生成装置３４０から出力された乱数を得る（ステップＢ３）。

【００７２】

乱数を受け取った条件分岐制御手段３２３は、受け取った乱数に依存して出力結果が同一となる複数の処理手続きの中から実際に行う処理手続きを選択等する乱数依存条件分岐決定操作を行う（ステップＢ４）。

【００７３】

暗号化演算手段３２１は、ステップＢ４の乱数依存条件分岐決定操作が終了した後に、またはステップＢ２で「条件分岐決定要求がない」と判定した場合には、暗号化処理を一段階実行する（ステップＢ５）。

【００７４】

暗号化演算手段３２１は、暗号化を一段階実行したことで暗号化処理が終了したか否かを判定する（ステップＢ６）。

【００７５】

暗号化演算手段３２１は、ステップＢ６で「暗号化を一段階実行したことで暗

号化処理が終了した」と判定した場合には、出力装置３５０に暗号文を出力し（ステップＢ７）、全体の処理を終了させる。

【００７６】

一方、暗号化演算手段３２１は、ステップＢ６で「暗号化処理が終了していない」と判定した場合（暗号化処理がまだ残されている場合）には、ステップＢ２に制御を戻して暗号化処理を継続させる。

【００７７】

次に、本実施の形態における効果について説明する。

【００７８】

本実施の形態では、乱数によって実行される暗号化処理の順序や種類が変化するために、特定の時刻に着目しても当該時刻において暗号化処理装置３２０の内部で行われている処理が乱数によって異なっており、消費電力の変化を観測しても当該消費電力の変化がどの暗号化処理に対応しているのかを判断することが困難になる。したがって、暗号化装置を電力解析や電力差分解析による暗号解析に対して耐性があるようにすることができる。

【００７９】

（３）　第３の実施の形態

図５は、本発明の第３の実施の形態に係る暗号化装置の構成を示すブロック図である。

【００８０】

図５を参照すると、本発明の実施の形態に係る暗号化装置は、入力装置５１０と、暗号化処理装置５２０と、記憶装置５３０と、乱数生成装置５４０と、出力装置５５０とを含んで構成されている。

【００８１】

これらの装置は、それぞれ、概略次のように動作する。

【００８２】

入力装置５１０は、暗号化処理の対象となる平文を暗号化処理装置５２０に対して供給する。

【００８３】

暗号化処理装置５２０は、乱数生成装置５４０から出力される乱数と入力装置５１０より入力される平文とを入力として、当該平文を暗号化処理装置５２０の内部に格納された鍵（暗号化鍵）で暗号化した暗号文を出力装置５５０から出力する。

【００８４】

ここで、暗号化処理装置５２０は、暗号化演算手段５２１と、乱数依存性決定手段５２２と、遅延制御手段５２３とを備えている。

【００８５】

暗号化演算手段５２１は、入力装置５１０を通して供給される平文を入力とし、暗号化演算手段５２１に格納されている暗号化鍵を用いて当該平文の暗号化を行う。暗号化演算手段５２１は、「遅延制御手段５２３による実行遅延時間の決定の乱数に依存した変更」を受けて状態を変化させつつ暗号化処理（複数の処理段階によって形成される暗号化処理）を実行し、最終的に当該平文を暗号化した暗号文を出力する。なお、暗号化演算手段５２１は、暗号化処理実行中の複数の時点で、暗号化演算手段５２１による暗号化処理の現在の処理段階を乱数依存性決定手段５２２に送る（これにより、適切な処理段階で乱数に依存した状態の変化を生じさせることができる）。

【００８６】

乱数依存性決定手段５２２は、暗号化演算手段５２１が出力する暗号化演算手段５２１の現在の処理段階を入力として、当該処理段階に基づいて遅延制御手段５２３に遅延時間決定要求を出力すべきか否かを判断し、「遅延時間決定要求の出力」を決定した場合（現在の処理段階が乱数に依存した操作を適用すべき処理段階であると判断した場合）には遅延制御手段５２３に遅延時間決定要求を出力する。

【００８７】

遅延制御手段５２３は、乱数依存性決定手段５２２より出力される遅延時間決定要求を入力した場合に、乱数生成装置５４０に乱数要求信号を送ることによって乱数を取得し、取得した乱数に依存して暗号化処理中に意図的に発生させる実行遅延の遅延時間を決定して当該遅延を挿入する操作（乱数依存遅延挿入操作）

を行う。

【００８８】

なお、遅延制御手段５２３は、暗号化演算手段５２１の処理に取得した乱数に応じた遅延を挿入する操作を行うように構成されており、遅延の挿入は暗号化に必要なデータにまったく乱数の影響をおよぼさない。したがって、最終的に出力される暗号文は、乱数生成手段５４０から出力される乱数に依存しない。

【００８９】

記憶装置５３０は、中間データ記憶部５３１を備えている。

【００９０】

中間データ記憶部５３１は、暗号化処理装置５２０が行う暗号化処理中に保持する必要のある中間データを格納する。

【００９１】

乱数生成装置５４０は、暗号化処理装置５２０より乱数要求信号を受け取り、当該乱数要求信号に基づいて暗号化処理装置５２０に乱数を出力する。

【００９２】

図６は、本実施の形態に係る暗号化装置の処理を示す流れ図である。この処理は、平文入力ステップＣ１と、遅延時間決定要求有無判定ステップＣ２と、乱数出力ステップＣ３と、乱数依存遅延挿入操作ステップＣ４と、暗号化処理一段階実行ステップＣ５と、暗号化処理終了判定ステップＣ６と、暗号文出力ステップＣ７とからなる。。

【００９３】

次に、図５および図６を参照して、本実施の形態に係る暗号化装置の全体の動作について詳細に説明する。

【００９４】

まず、暗号化を行いたい平文が、入力装置５１０から暗号化処理装置５２０内の暗号化演算手段５２１に入力される（図６のステップＣ１）。

【００９５】

暗号化演算手段５２１は、暗号化演算手段５２１における暗号化処理の現在の処理段階を乱数依存性決定手段５２２に出力する。

【００９６】

乱数依存性決定手段５２２は、暗号化演算手段５２１より受け取った暗号化演算手段５２１の処理段階に関する情報を基に、現在の処理段階が乱数に依存した遅延を挿入する処理段階（当該遅延の遅延時間を決定する処理段階）であるか否かの判断を行い、「乱数に依存した遅延を挿入する処理段階である」と判断した場合には遅延制御手段５２３に遅延時間決定要求を出力する。

【００９７】

遅延制御手段５２３は、乱数依存性決定手段５２２からの遅延時間決定要求があるか否かを判定する（ステップＣ２）。

【００９８】

遅延制御手段５２３は、ステップＣ２で「遅延時間決定要求がある」と判定した場合には、当該遅延時間決定要求を受け取り、乱数要求（乱数要求信号）を乱数生成装置５４０に送り、当該乱数要求信号に基づいて乱数生成装置５４０から出力された乱数を得る（ステップＣ３）。

【００９９】

乱数を受け取った遅延制御手段５２３は、受け取った乱数に依存して遅延時間を決定し、決定した遅延時間の実行遅延を暗号化処理中に意図的に挿入する（ステップＣ４）。

【０１００】

暗号化演算手段５２１は、ステップＣ４の乱数依存遅延挿入操作が終了した後に、またはステップＢ２で「乱数依存遅延時間決定要求がない」と判定した場合には、暗号化処理を一段階実行する（ステップＣ５）。

【０１０１】

暗号化演算手段５２１は、暗号化を一段階実行したことで暗号化処理が終了したか否かを判定する（ステップＣ６）。

【０１０２】

暗号化演算手段５２１は、ステップＣ６で「暗号化を一段階実行したことで暗号化処理が終了した」と判定した場合には、出力装置５５０に暗号文を出力し（ステップＣ７）、全体の処理を終了させる。

【０１０３】

一方、暗号化演算手段５２１は、ステップＣ６で「暗号化処理が終了していない」と判定した場合（暗号化処理がまだ残されている場合）には、ステップＣ２に制御を戻して暗号化処理を継続させる。

【０１０４】

次に、本実施の形態における効果について説明する。

【０１０５】

本実施の形態では、乱数に依存した遅延時間の実行遅延が適宜挿入されるために、暗号解析に有用となる処理が行われている時刻が絶えず変化し、どの時刻の消費電力の変化に着目すれば効率的に暗号解析に必要な情報を得ることができるのかを特定することが困難になる。したがって、暗号化装置を電力解析や電力差分解析による暗号解析に対して耐性があるようにすることができる。

【０１０６】

なお、上述の第１，第２，および第３の実施の形態に係る暗号化装置においては、暗号化鍵が予め暗号化演算手段（図１中の暗号化演算手段１２１，図３中の暗号化演算手段３２１，および図５中の暗号化演算手段５２１）に格納されていた。

【０１０７】

しかし、入力装置（図１中の入力装置１１０，図３中の入力装置３１０，および図５中の入力装置５１０）から暗号化演算手段に暗号化鍵を入力するように、上記の暗号化装置を構成することも可能である。この場合には、暗号化鍵を入力された暗号化演算手段は、その後に入力される１つまたは複数の平文の暗号化を当該暗号化鍵を用いて行い、暗号文を出力する。

【０１０８】

上記のような構成を採用すると、暗号化鍵を外部から入力するようにできるため、暗号化演算手段自体を変更せずに暗号化鍵の更新を容易に行うことができるようになる。

【０１０９】

また、上述の第１，第２，および第３の実施の形態に係る暗号化装置において

は、乱数生成装置（図１中の乱数生成装置１４０，図３中の乱数生成装置３４０，および図５中の乱数生成装置５４０）から出力される乱数を、入力装置から暗号化処理装置（図１中の暗号化処理装置１２０，図３中の暗号化処理装置３２０，および図５中の暗号化処理装置５２０）に入力されるデータ（平文）そのものまたは当該データに依存したデータとすることも可能である。

【０１１０】

このように平文を「乱数」として使用することが可能かつ有効になるのは、現在提案されている電力解析および電力差分解析では暗号文と消費電力とのみから暗号解析が行われており、平文のデータは暗号解析に使用されていないため、平文を乱数として利用することができるからである。なお、乱数として「平文に依存したデータ」を用いるということは、例えば入力装置に入力される平文を暗号化鍵とは別の「乱数出力用鍵」で暗号化し、その暗号化の出力を乱数として利用するという暗号化装置も、本発明に含まれることになる。

【０１１１】

（４）　第４の実施の形態

図７は、本発明の第４の実施の形態に係る暗号化装置の構成を示すブロック図である。

【０１１２】

図７を参照すると、本発明の第４の実施の形態に係る暗号化装置は、図１に示した第１の実施の形態に係る暗号化装置に対して、暗号化処理プログラムを記録した記録媒体７００を備える点が異なっている。この記録媒体７００は、磁気ディスク，半導体メモリ，ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ　Ｄｉｓｋ－Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ），その他の記録媒体であってよい。

【０１１３】

暗号化処理プログラムは、記録媒体７００からコンピュータシステム（入力装置１１０，暗号化処理装置１２０，記憶装置１３０，乱数生成装置１４０，および出力装置１５０を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置１１０，暗号化処理装置１２０（暗号化演算手段１２１，乱数依存性決定手段１２２，および中間データ制御手段１２３），記憶

装置１３０（中間データ記憶部１３１），乱数生成装置１４０，および出力装置１５０として制御する。暗号化処理プログラムの制御による入力装置１１０，暗号化処理装置１２０，記憶装置１３０，乱数生成装置１４０，および出力装置１５０の動作は、第１の実施の形態における入力装置１１０，暗号化処理装置１２０，記憶装置１３０，乱数生成装置１４０，および出力装置１５０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１１４】

（５）　第５の実施の形態

図８は、本発明の第５の実施の形態に係る暗号化装置の構成を示すブロック図である。

【０１１５】

図８を参照すると、本発明の第５の実施の形態に係る暗号化装置は、図３に示した第２の実施の形態に係る暗号化装置に対して、暗号化処理プログラムを記録した記録媒体８００を備える点が異なっている。この記録媒体８００は、磁気ディスク，半導体メモリ，ＣＤ－ＲＯＭ，その他の記録媒体であってよい。

【０１１６】

暗号化処理プログラムは、記録媒体８００からコンピュータシステム（入力装置３１０，暗号化処理装置３２０，記憶装置３３０，乱数生成装置３４０，および出力装置３５０を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置３１０，暗号化処理装置３２０（暗号化演算手段３２１，乱数依存性決定手段３２２，および条件分岐制御手段３２３），記憶装置３３０（中間データ記憶部３３１），乱数生成装置３４０，および出力装置３５０として制御する。暗号化処理プログラムの制御による入力装置３１０，暗号化処理装置３２０，記憶装置３３０，乱数生成装置３４０，および出力装置３５０の動作は、第２の実施の形態における入力装置３１０，暗号化処理装置３２０，記憶装置３３０，乱数生成装置３４０，および出力装置３５０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１１７】

（６）　第６の実施の形態

図９は、本発明の第６の実施の形態に係る暗号化装置の構成を示すブロック図である。

【０１１８】

図９を参照すると、本発明の第６の実施の形態に係る暗号化装置は、図５に示した第３の実施の形態に係る暗号化装置に対して、暗号化処理プログラムを記録した記録媒体９００を備える点が異なっている。この記録媒体９００は、磁気ディスク，半導体メモリ，ＣＤ－ＲＯＭ，その他の記録媒体であってよい。

【０１１９】

暗号化処理プログラムは、記録媒体９００からコンピュータシステム（入力装置５１０，暗号化処理装置５２０，記憶装置５３０，乱数生成装置５４０，および出力装置５５０を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置５１０，暗号化処理装置５２０（暗号化演算手段５２１，乱数依存性決定手段５２２，および遅延制御手段５２３），記憶装置５３０（中間データ記憶部５３１），乱数生成装置５４０，および出力装置５５０として制御する。暗号化処理プログラムの制御による入力装置５１０，暗号化処理装置５２０，記憶装置５３０，乱数生成装置５４０，および出力装置５５０の動作は、第３の実施の形態における入力装置５１０，暗号化処理装置５２０，記憶装置５３０，乱数生成装置５４０，および出力装置５５０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１２０】

（７）　第７の実施の形態

図１０は、本発明の第７の実施の形態に係る復号装置の構成を示すブロック図である。

【０１２１】

図１０を参照すると、本実施の形態に係る復号装置は、入力装置１０１０と、復号演算手段１０２１，乱数依存性決定手段１０２２，および中間データ制御手段１０２３を備える復号処理装置１０２０と、中間データ記憶部１０３１を備える記憶装置１０３０と、乱数生成装置１０４０と、出力装置１０５０とを含んで構成されている。

【０１２２】

本実施の形態に係る復号装置は、第１の実施の形態に係る暗号化装置と同様に、入力装置，復号処理装置（暗号化処理装置に該当する），記憶装置，乱数生成装置，および出力装置を備えている。ここで、第１の実施の形態では、入力装置１１０からは平文が入力され、暗号化処理装置１２０が暗号化鍵を用いて平文の暗号化を行い、出力装置１５０から暗号文が出力されていた。これに対し、本実施の形態では、入力装置１０１０からは暗号文が入力され、復号処理装置１０２０が復号鍵を用いて暗号文の復号を行い、出力装置１０５０から平文が出力される。上記の点で、本実施の形態に係る復号装置は第１の実施の形態に係る暗号化装置と異なっている（それ以外の構成や動作は同様である）。

【０１２３】

（８）　第８の実施の形態

図１１は、本発明の第８の実施の形態に係る復号装置の構成を示すブロック図である。

【０１２４】

図１１を参照すると、本実施の形態に係る復号装置は、入力装置１１１０と、復号演算手段１１２１，乱数依存性決定手段１１２２，および条件分岐制御手段１１２３を備える復号処理装置１１２０と、中間データ記憶部１１３１を備える記憶装置１１３０と、乱数生成装置１１４０と、出力装置１１５０とを含んで構成されている。

【０１２５】

本実施の形態に係る復号装置は、第２の実施の形態に係る暗号化装置と同様に、入力装置，復号処理装置（暗号化処理装置に該当する），記憶装置，乱数生成装置，および出力装置を備えている。ここで、第２の実施の形態では、入力装置３１０からは平文が入力され、暗号化処理装置３２０が暗号化鍵を用いて平文の暗号化を行い、出力装置３５０から暗号文が出力されていた。これに対し、本実施の形態では、入力装置１１１０からは暗号文が入力され、復号処理装置１１２０が復号鍵を用いて暗号文の復号を行い、出力装置１１５０から平文が出力される。上記の点で、本実施の形態に係る復号装置は第２の実施の形態に係る暗号化

装置と異なっている（それ以外の構成や動作は同様である）。

【０１２６】

（９）　第９の実施の形態

図１２は、本発明の第９の実施の形態に係る復号装置の構成を示すブロック図である。

【０１２７】

図１２を参照すると、本実施の形態に係る復号装置は、入力装置１２１０と、復号演算手段１２２１，乱数依存性決定手段１２２２，および遅延制御手段１２２３を備える復号処理装置１２２０と、中間データ記憶部１２３１を備える記憶装置１２３０と、乱数生成装置１２４０と、出力装置１２５０とを含んで構成されている。

【０１２８】

本実施の形態に係る復号装置は、第３の実施の形態に係る暗号化装置と同様に、入力装置，復号処理装置（暗号化処理装置に該当する），記憶装置，乱数生成装置，および出力装置を備えている。ここで、第３の実施の形態では、入力装置５１０からは平文が入力され、暗号化処理装置５２０が暗号化鍵を用いて平文の暗号化を行い、出力装置５５０から暗号文が出力されていた。これに対し、本実施の形態では、入力装置１２１０からは暗号文が入力され、復号処理装置１２２０が復号鍵を用いて暗号文の復号を行い、出力装置１２５０から平文が出力される。上記の点で、本実施の形態に係る復号装置は第３の実施の形態に係る暗号化装置と異なっている（それ以外の構成や動作は同様である）。

【０１２９】

なお、上述の第７，第８，および第９の実施の形態に係る復号装置においては、入力装置（図１０中の入力装置１０１０，図１１中の入力装置１１１０，および図１２中の入力装置１２１０）から復号演算手段（図１０中の復号演算手段１０２１，図１１中の復号演算手段１１２１，および図１２中の復号演算手段１２２１）に復号鍵を入力するように構成することも可能である。

【０１３０】

また、上述の第７，第８，および第９の実施の形態に係る復号装置においては

、乱数生成装置（図１０中の乱数生成装置１０４０，図１１中の乱数生成装置１１４０，および図１２中の乱数生成装置１２４０）から出力される乱数を、入力装置から復号処理装置（図１０中の復号処理装置１０２０，図１１中の復号処理装置１１２０，および図１２中の復号処理装置１２２０）に入力されるデータ（暗号文）そのものまたは当該データに依存したデータとすることも可能である。

【０１３１】

（１０）　第１０の実施の形態

図１３は、本発明の第１０の実施の形態に係る復号装置の構成を示すブロック図である。

【０１３２】

図１３を参照すると、本発明の第１０の実施の形態に係る復号装置は、図１０に示した第７の実施の形態に係る復号装置に対して、復号処理プログラムを記録した記録媒体１３００を備える点が異なっている。この記録媒体１３００は、磁気ディスク，半導体メモリ，ＣＤ－ＲＯＭ，その他の記録媒体であってよい。

【０１３３】

復号処理プログラムは、記録媒体１３００からコンピュータシステム（入力装置１０１０，復号処理装置１０２０，記憶装置１０３０，乱数生成装置１０４０，および出力装置１０５０を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置１０１０，復号処理装置１０２０（復号演算手段１０２１，乱数依存性決定手段１０２２，および中間データ制御手段１０２３），記憶装置１０３０（中間データ記憶部１０３１），乱数生成装置１０４０，および出力装置１０５０として制御する。復号処理プログラムの制御による入力装置１０１０，復号処理装置１０２０，記憶装置１０３０，乱数生成装置１０４０，および出力装置１０５０の動作は、第７の実施の形態における入力装置１０１０，復号処理装置１０２０，記憶装置１０３０，乱数生成装置１０４０，および出力装置１０５０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１３４】

（１１）　第１１の実施の形態

図１４は、本発明の第１１の実施の形態に係る復号装置の構成を示すブロック図である。

【０１３５】

図１４を参照すると、本発明の第１１の実施の形態に係る復号装置は、図１１に示した第８の実施の形態に係る復号装置に対して、復号処理プログラムを記録した記録媒体１４００を備える点が異なっている。この記録媒体１４００は、磁気ディスク，半導体メモリ，ＣＤ－ＲＯＭ，その他の記録媒体であってよい。

【０１３６】

復号処理プログラムは、記録媒体１４００からコンピュータシステム（入力装置１１１０，復号処理装置１１２０，記憶装置１１３０，乱数生成装置１１４０，および出力装置１１５０を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置１１１０，復号処理装置１１２０（復号演算手段１１２１，乱数依存性決定手段１１２２，および条件分岐制御手段１１２３），記憶装置１１３０（中間データ記憶部１１３１），乱数生成装置１１４０，および出力装置１１５０として制御する。復号処理プログラムの制御による入力装置１１１０，復号処理装置１１２０，記憶装置１１３０，乱数生成装置１１４０，および出力装置１１５０の動作は、第８の実施の形態における入力装置１１１０，復号処理装置１１２０，記憶装置１１３０，乱数生成装置１１４０，および出力装置１１５０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１３７】

（１２）　第１２の実施の形態

図１５は、本発明の第１２の実施の形態に係る復号装置の構成を示すブロック図である。

【０１３８】

図１５を参照すると、本発明の第１２の実施の形態に係る復号装置は、図１２に示した第９の実施の形態に係る復号装置に対して、復号処理プログラムを記録した記録媒体１５００を備える点が異なっている。この記録媒体１５００は、磁

気ディスク，半導体メモリ，ＣＤ－ＲＯＭ，その他の記録媒体であってよい。

【０１３９】

復号処理プログラムは、記録媒体１５００からコンピュータシステム（入力装置１２１０，復号処理装置１２２０，記憶装置１２３０，乱数生成装置１２４０，および出力装置１２５０を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置１２１０，復号処理装置１２２０（復号演算手段１２２１，乱数依存性決定手段１２２２，および遅延制御手段１２２３），記憶装置１２３０（中間データ記憶部１２３１），乱数生成装置１２４０，および出力装置１２５０として制御する。復号処理プログラムの制御による入力装置１２１０，復号処理装置１２２０，記憶装置１２３０，乱数生成装置１２４０，および出力装置１２５０の動作は、第９の実施の形態における入力装置１２１０，復号処理装置１２２０，記憶装置１２３０，乱数生成装置１２４０，および出力装置１２５０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１４０】

（１３）　第１３の実施の形態

図１６は、本発明の第１３の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【０１４１】

図１６を参照すると、本実施の形態に係る暗号化・復号装置は、入力装置１６１０と、暗号化・復号演算手段１６２１，乱数依存性決定手段１６２２，および中間データ制御手段１６２３を備える暗号化・復号処理装置１６２０と、中間データ記憶部１６３１を備える記憶装置１６３０と、乱数生成装置１６４０と、出力装置１６５０とを含んで構成されている。

【０１４２】

本実施の形態に係る暗号化・復号装置は、第１の実施の形態に係る暗号化装置の機能と第７の実施の形態に係る復号装置の機能とを併有している。ここで、入力装置１６１０，乱数依存性決定手段１６２２，中間データ制御手段１６２３，記憶装置１６３０，乱数生成装置１６４０，および出力装置１６５０は、第１の

実施の形態や第７の実施における同名の構成要素と同様のものである。

【０１４３】

暗号化・復号演算手段１６２１は、処理データおよび処理内容を入力とし、中間データ制御手段１６２３による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって乱数生成装置１６４０の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって乱数生成装置１６４０の出力に依存しない平文を出力する。

【０１４４】

（１４）　第１４の実施の形態

図１７は、本発明の第１４の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【０１４５】

図１７を参照すると、本実施の形態に係る暗号化・復号装置は、入力装置１７１０と、暗号化・復号演算手段１７２１，乱数依存性決定手段１７２２，および条件分岐制御手段１７２３を備える暗号化・復号処理装置１７２０と、中間データ記憶部１７３１を備える記憶装置１７３０と、乱数生成装置１７４０と、出力装置１７５０とを含んで構成されている。

【０１４６】

本実施の形態に係る暗号化・復号装置は、第２の実施の形態に係る暗号化装置の機能と第８の実施の形態に係る復号装置の機能とを併有している。ここで、入力装置１７１０，乱数依存性決定手段１７２２，条件分岐制御手段１７２３，記憶装置１７３０，乱数生成装置１７４０，および出力装置１７５０は、第２の実施の形態や第８の実施における同名の構成要素と同様のものである。

【０１４７】

暗号化・復号演算手段１７２１は、処理データおよび処理内容を入力とし、条件分岐制御手段１７２３による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であっ

た場合には当該処理データである平文を暗号化した暗号文であって乱数生成装置１７４０の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって乱数生成装置１７４０の出力に依存しない平文を出力する。

【０１４８】

（１５）　第１５の実施の形態

図１８は、本発明の第１５の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【０１４９】

図１８を参照すると、本実施の形態に係る暗号化・復号装置は、入力装置１８１０と、暗号化・復号演算手段１８２１，乱数依存性決定手段１８２２，および遅延制御手段１８２３を備える暗号化・復号処理装置１８２０と、中間データ記憶部１８３１を備える記憶装置１８３０と、乱数生成装置１８４０と、出力装置１８５０とを含んで構成されている。

【０１５０】

本実施の形態に係る暗号化・復号装置は、第３の実施の形態に係る暗号化装置の機能と第９の実施の形態に係る復号装置の機能とを併有している。ここで、入力装置１８１０，乱数依存性決定手段１８２２，遅延制御手段１８２３，記憶装置１８３０，乱数生成装置１８４０，および出力装置１８５０は、第３の実施の形態や第９の実施における同名の構成要素と同様のものである。

【０１５１】

暗号化・復号演算手段１８２１は、処理データおよび処理内容を入力とし、遅延制御手段１８２３による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって乱数生成装置１８４０の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって乱数生成装置１８４０の出力に依存しない平文を出力する。

【０１５２】

なお、上述の第１３，第１４，および第１５の実施の形態に係る暗号化・復号装置においては、入力装置（図１６中の入力装置１６１０，図１７中の入力装置１７１０，および図１８中の入力装置１８１０）から暗号化・復号演算手段（図１６中の暗号化・復号演算手段１６２１，図１７中の暗号化・復号演算手段１７２１，および図１８中の暗号化・復号演算手段１８２１）に暗号化鍵および復号鍵を入力するように構成することも可能である。

【０１５３】

また、上述の第１３，第１４，および第１５の実施の形態に係る暗号化・復号装置においては、乱数生成装置（図１６中の乱数生成装置１６４０，図１７中の乱数生成装置１７４０，および図１８中の乱数生成装置１８４０）から出力される乱数を、入力装置から暗号化・復号処理装置（図１６中の暗号化・復号処理装置１６２０，図１７中の暗号化・復号処理装置１７２０，および図１８中の暗号化・復号処理装置１８２０）に入力されるデータ（暗号文または平文）そのものまたは当該データに依存したデータとすることも可能である。

【０１５４】

（１６）　第１６の実施の形態

図１９は、本発明の第１６の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【０１５５】

図１９を参照すると、本発明の第１６の実施の形態に係る暗号化・復号装置は、図１６に示した第１３の実施の形態に係る暗号化・復号装置に対して、暗号化・復号処理プログラムを記録した記録媒体１９００を備える点が異なっている。この記録媒体１９００は、磁気ディスク，半導体メモリ，ＣＤ－ＲＯＭ，その他の記録媒体であってよい。

【０１５６】

暗号化・復号処理プログラムは、記録媒体１９００からコンピュータシステム（入力装置１６１０，暗号化・復号処理装置１６２０，記憶装置１６３０，乱数生成装置１６４０，および出力装置１６５０を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置１６１０，暗号化・復

号処理装置１６２０（暗号化・復号演算手段１６２１，乱数依存性決定手段１６２２，および中間データ制御手段１６２３），記憶装置１６３０（中間データ記憶部１６３１），乱数生成装置１６４０，および出力装置１６５０として制御する。暗号化・復号処理プログラムの制御による入力装置１６１０，暗号化・復号処理装置１６２０，記憶装置１６３０，乱数生成装置１６４０，および出力装置１６５０の動作は、第１３の実施の形態における入力装置１６１０，暗号化・復号処理装置１６２０，記憶装置１６３０，乱数生成装置１６４０，および出力装置１６５０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１５７】

（１７）　第１７の実施の形態

図２０は、本発明の第１７の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【０１５８】

図２０を参照すると、本発明の第１７の実施の形態に係る暗号化・復号装置は、図１７に示した第１４の実施の形態に係る暗号化・復号装置に対して、暗号化・復号処理プログラムを記録した記録媒体２０００を備える点が異なっている。この記録媒体２０００は、磁気ディスク，半導体メモリ，ＣＤ－ＲＯＭ，その他の記録媒体であってよい。

【０１５９】

暗号化・復号処理プログラムは、記録媒体２０００からコンピュータシステム（入力装置１７１０，暗号化・復号処理装置１７２０，記憶装置１７３０，乱数生成装置１７４０，および出力装置１７５０を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置１７１０，暗号化・復号処理装置１７２０（暗号化・復号演算手段１７２１，乱数依存性決定手段１７２２，および条件分岐制御手段１７２３），記憶装置１７３０（中間データ記憶部１７３１），乱数生成装置１７４０，および出力装置１７５０として制御する。暗号化・復号処理プログラムの制御による入力装置１７１０，暗号化・復号処理装置１７２０，記憶装置１７３０，乱数生成装置１７４０，および出力装置１７５０の動作は、第１４の実施の形態における入力装置１７１０，暗号化・復号

処理装置１７２０，記憶装置１７３０，乱数生成装置１７４０，および出力装置１７５０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１６０】

（１８）　第１８の実施の形態

図２１は、本発明の第１８の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【０１６１】

図２１を参照すると、本発明の第１８の実施の形態に係る暗号化・復号装置は、図１８に示した第１５の実施の形態に係る暗号化・復号装置に対して、暗号化・復号処理プログラムを記録した記録媒体２１００を備える点が異なっている。この記録媒体２１００は、磁気ディスク，半導体メモリ，ＣＤ－ＲＯＭ，その他の記録媒体であってよい。

【０１６２】

暗号化・復号処理プログラムは、記録媒体２１００からコンピュータシステム（入力装置１８１０，暗号化・復号処理装置１８２０，記憶装置１８３０，乱数生成装置１８４０，および出力装置１８５０を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置１８１０，暗号化・復号処理装置１８２０（暗号化・復号演算手段１８２１，乱数依存性決定手段１８２２，および遅延制御手段１８２３），記憶装置１８３０（中間データ記憶部１８３１），乱数生成装置１８４０，および出力装置１８５０として制御する。暗号化・復号処理プログラムの制御による入力装置１８１０，暗号化・復号処理装置１８２０，記憶装置１８３０，乱数生成装置１８４０，および出力装置１８５０の動作は、第１５の実施の形態における入力装置１８１０，暗号化・復号処理装置１８２０，記憶装置１８３０，乱数生成装置１８４０，および出力装置１８５０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１６３】

【実施例】

次に、本発明の実施例を、図面を参照して説明する。

【０１６４】

（１）　第１の実施例

図２２および図２３は、本発明の第１の実施例を説明するための図である。

【０１６５】

本実施例は、上述の第１の実施の形態に係る暗号化装置を、共通鍵暗号ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）対応とするものである。

【０１６６】

なお、ＤＥＳ暗号については、『「Ｈａｎｄｂｏｏｋ　ｏｆ　Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ」（Ａ．Ｍｅｎｅｚｅｓ，Ｐ．Ｏｏｒｓｃｈｏｔ，Ｓ．Ｖａｎｓｔｏｎｅ著，ＣＲＣ　Ｐｒｅｓｓ，１９９７，ＩＳＢＮ　０－８４９３－８５２３－７）ｐｐ．２５０－２５９』に詳しく述べられている。

【０１６７】

ここでは、まず、図２２を用いてＤＥＳの動作の概要を示す。

【０１６８】

ＤＥＳは、鍵スケジューリング部２２１０と、データ処理部２２２０とを備えている。鍵スケジューリング部２２１０は、６４ビットの暗号化鍵を入力とし、１６個の４８ビット中間鍵K_1～K_{16}を出力する。データ処理部２２２０は、初期転置ＩＰと、最終転置IP^{-1}と、１６個のＦ関数とを備えており、６４ビットの平文と鍵スケジューリング部２２１０から出力される１６個の４８ビットの中間鍵K_1～K_{16}を入力とし、６４ビットの暗号文を出力する。ここでＩＰおよびIP^{-1}は予め定められているビットの並び替えを行う関数であり、１６個のＦ関数は３２ビットのデータと４８ビットのデータとを入力とし３２ビットのデータを出力する予め定められた関数である。

【０１６９】

平文の暗号化は次のように行われる。

【０１７０】

まず、平文は、初期転置ＩＰが施された後に、上位３２ビットL_0と下位３２ビットR_0とに分割される。このL_0およびR_0から、次式に従ってL_1，R_1，L_2，R_2，L_3，R_3，…，L_{15}，R_{15}，L_{16}，R_{16}が生成される。なお、

上記のL_0，R_0，L_1，R_1，…が、図１中の中間データ記憶部１３１内の中間データに該当する。

【０１７１】

【数１】

$$L_n = R_{n-1}$$
$$R_n = L_{n-1} \oplus F(R_{n-1}, K_n) \quad \text{(但し} \oplus \text{はビット毎の排他的論理和)}$$

【０１７２】

ここで、ｎ＝１，２，…，１６である。なお、上式の記号Ｆは、ＤＥＳのＦ関数を表している。

【０１７３】

ＤＥＳの１６個のＦ関数は、どれも同じ構造を持ち、３２ビットのデータR_{n-1}と鍵スケジューリング部２２１０より出力される４８ビットの中間鍵K_nとを入力とし、３２ビットのデータを出力する。上式を１６回適用することによって得られたL_{16}を上位３２ビットとし、R_{16}を下位３２ビットとする６４ビットのデータに対して最終転置IP^{-1}を施すことによって、６４ビットの暗号文が得られる。

【０１７４】

図２３に、本実施例の概念を示す。

【０１７５】

図２３において破線で囲まれた部分（図２３中の２３１０～２３８０）が、ＤＥＳの暗号化の過程で必要になる中間データの変化に乱数依存性を持たせている部分（乱数依存性付与部分）である。すなわち、当該乱数依存性付与部分が、図１中の中間データ制御手段１２３により行われる乱数依存中間データ変更操作を表している。

【０１７６】

以下に、図２２および図２３を基に、本実施例の構成および動作について説明する。

【０１７７】

まず初めに、入力装置であるＩＣカード・リーダ・ライタより平文が入力され

る。平文は初期転置ＩＰが施された後に、上位３２ビットと下位３２ビットとに分けられる。この時点で中間データ制御手段が呼び出される。中間データ制御手段は、乱数生成装置から２つの乱数r_0およびr_1を受け取り、上位３２ビットのデータと乱数r_0との排他的論理和をとった結果をL_0に格納し（図２３の２３１０参照）、下位３２ビットのデータと乱数r_1との排他的論理和をとった結果をR_0に格納する（図２３の２３２０参照）。

【０１７８】

次に、ｎ＝１，２，…，１６に対し、以下の操作が繰り返される。ただし、以下に現れるr^*の値は次のように定義される。

【０１７９】

【数２】

$$r^* = \begin{cases} r_1 & (n = 1,4,7,10,13,16 \text{ の時}) \\ r_0 \oplus r_1 & (n = 2,5,8,11,14 \text{ の時}) \\ r_0 & (n = 3,6,9,12,15 \text{ の時}) \end{cases}$$

【０１８０】

まず、R_{n-1}の値がL_nに複写される。続いて、再び中間データ制御手段が呼び出され、R_{n-1}とr^*との排他的論理和がとられる（図２３の２３４０，２３６０，および２３８０参照）。この排他的論理和の値とK_nとが、Ｆ関数への入力とされる。以上の手続きにより、Ｆ関数への入力はR_{n-1}とK_nとなり、乱数生成装置から出力される乱数r^*に依存していないことが確かめられる。

【０１８１】

Ｆ関数の値が出力されると、中間データ制御手段が呼び出され、再びＦ関数の出力と乱数r^*との排他的論理和がとられる（図２３の２３３０，２３５０，および２３７０参照）。さらに、その結果とL_{n-1}との排他的論理和が計算され、計算結果がL_nに格納される。

【０１８２】

上記操作を１６回繰り返すことによって得られるL_{16}とr_1との排他的論理和をとった値を上位３２ビットとし、R_{16}とr_0とr_1との排他的論理和をとった値を下位３２ビットとする６４ビットのデータに、最終転置IP^{-1}が施された６４ビットのデータが、暗号文としてＩＣカード・リーダ・ライタを通して出力

される。

【０１８３】

このとき得られる暗号文は、中間データを操作する乱数r_0およびr_1，遅延時間を制御する乱数，ならびにＳ－ｂｏｘの実行順序を決定する乱数のいずれの乱数にも依存しないデータになっている。

【０１８４】

（２）　第２の実施例

図２４，図２５，および図２６は、本発明の第２の実施例を説明するための図である。

【０１８５】

本実施例は、上述の第２の実施の形態に係る暗号化装置を、共通鍵暗号ＲＣ５－３２／１２／１６に適用したものである。

【０１８６】

なお、ＲＣ５－３２／１２／１６のアルゴリズムの詳細に関しては、上記の「Ｈａｎｄｂｏｏｋ　ｏｆ　Ａｐｐｌｉｅｄ　Ｃｒｙｐｔｏｇｒａｐｈｙ」のｐｐ．２６９－２７０に述べられている。

【０１８７】

ここでは、まず、図２４および図２５を参照して、ＲＣ５－３２／１２／１６の動作を概説する。

【０１８８】

ＲＣ５－３２／１２／１６は、図２４に示すように、１２８ビットの暗号化鍵２４２０を用いて６４ビットの平文２４１０を６４ビットの暗号文２４５０に変換するアルゴリズムである。

【０１８９】

ＲＣ５－３２／１２／１６は、データ処理部２４３０と、拡大鍵生成部２４４０とを有している。

【０１９０】

拡大鍵生成部２４４０は、１２８ビットの暗号化鍵２４２０を入力とし、２６個の３２ビットの拡大鍵S_0，S_1，…，S_{25}を出力する。

【0191】

データ処理部2430は、64ビットの平文2410と、拡大鍵生成部2440の出力S_0，S_1，…，S_{25}とを入力とし、64ビットの暗号文2450を出力する。

【0192】

データ処理部2430は、次のように動作する。

【0193】

まず、入力された64ビットの平文2410は、上位32ビットAと下位32ビットBとに分割される。次に、AとS_0との2^{32}を法とする和（加算）がとられ、その結果が再びAに代入される（図24の2431参照）。また、BとS_1との2^{32}を法とする和がとられ、その結果が再びBに代入される（図24の2432参照）。その後、AおよびBは、ラウンド関数と呼ばれる変換を12回適用される。

【0194】

暗号文2450は、ラウンド関数を12回適用した後のAを上位32ビットとして持ち、Bを下位32ビットとして持つ64ビットのデータとなる。

【0195】

第i回目に適用されるラウンド関数は、A，B，S_{2i}，およびS_{2i+1}を入力としてAおよびBのデータの更新を行い、更新されたAおよびBを出力する。

【0196】

次に、第i回目に適用されるラウンド関数の概要を説明する。

【0197】

第i回目に適用されるラウンド関数によるAおよびBの更新は、次式に従って行われる。

【0198】

【数3】

$$A = ((A \oplus B) \lll B) + S_{2i}$$
$$B = ((B \oplus A) \lll A) + S_{2i+1}$$

【0199】

ここで、「＋」は2^{32}を法とする和を表し、「Ｘ＜＜＜Ｙ」はＸのＹビット回転を表している。

【０２００】

図２５を参照すると、初めに、Ａの更新が行われる。まず、入力ＡはＢとビット毎の排他的論理和２５１０をとられ、その結果がＡに再び格納される。次に、Ａは、Ｂビットの左ビット回転２５２０を施され、その結果が再びＡに格納される。最後に、Ａと拡大鍵S_{2i}との2^{32}を法とする和２５３０がとられ、その結果が更新後のＡの値となる。

【０２０１】

続いて、Ｂの更新が行われる。まず、Ｂは、更新後のＡとビット毎の排他的論理和２５４０をとられ、その結果がＢに再び格納される。次に、Ｂは、Ａビットの左ビット回転２５５０を施され、その結果が再びＢに格納される。最後に、Ｂと拡大鍵S_{2i+1}との2^{32}を法とする和２５６０がとられ、その結果が更新後のＢの値となる。

【０２０２】

本実施例は、入力装置および出力装置としてＩＣカード・リーダ・ライタを、データ記憶装置およびプログラムを格納した記憶媒体として半導体メモリを、暗号化処理装置としてＩＣカードに内蔵されたコンピュータを備えている。暗号化処理装置を実現するコンピュータは、汎用レジスタを５本以上有しており、また当該コンピュータの命令セットは、２つのレジスタＲ１，Ｒ２の算術和、ビット回転、ビット毎の排他的論理和等を計算した結果を必ずＲ１またはＲ２に格納するという特徴を有しているものとする。ちなみに、現在使用されているコンピュータの多くは、上記のような特徴を持つ命令セットを有している。

【０２０３】

次に、図２６の流れ図と図２４および図２５とを基に、本実施例の全体的な動作について詳細に説明する。

【０２０４】

図２６の流れ図において、Ｒ１，Ｒ２，Ｒ３，Ｒ４およびＲ５はデータ幅３２ビットの汎用レジスタを表しており、また表記「Ｒｉ←Ｒｉ＋Ｒｊ」は汎用レジ

スタＲｉとＲｊとを加算した結果を新たに汎用レジスタＲｉに格納する操作を表している。図２６中の「Ｒｉ←Ｒｉ＜＜＜Ｒｊ」等についても同様に解釈するものとする。

【０２０５】

本実施例は、コンピュータが行う「Ｒｉ＋Ｒｊ」および「Ｒｉ＜＜＜Ｒｊ」等のレジスタ間演算の演算結果をＲｉおよびＲｊのどちらに格納するかを乱数に依存して変化させることを特徴としている。

【０２０６】

演算結果の格納先を乱数に依存して変化させることで、電力を測定した場合の消費電力の変化が、汎用レジスタＲｉの値の変化によるものなのか、汎用レジスタＲｊの値の変化によるものなのかを検知することが困難になる。

【０２０７】

次に、本実施例の動作の詳細な説明を行う。

【０２０８】

本実施例では、まず初めに、入力装置を通じて暗号化処理装置に平文が格納される（図２６のステップＤ１）。

【０２０９】

平文が暗号化処理装置に入力されると、暗号化処理装置は汎用レジスタＲ１に加算（2^{32}を法とする和）２４３１が終了した後のＡの値を格納し、汎用レジスタＲ３に加算（2^{32}を法とする和）２４３２が終了した後のＢの値を格納する。また、ラウンド関数の実行回数をカウントする変数ｒに１を格納する（ステップＤ２）。

【０２１０】

次に、暗号化処理装置は、図２５に示されるラウンド関数の２５１０および２５２０に対応する操作を実行し、さらに汎用レジスタＲ２にS_{2r}を格納する。

【０２１１】

この時点で、条件分岐制御手段が呼び出され、Ｒ２の保持するS_{2r}の値とＲ１の保持するＡの値との和（2^{32}を法とする和）２５３０をとった計算結果をＲ１およびＲ２のどちらに格納するかを乱数の値の偶奇数に応じて変化させる（ステ

ップＤ３およびＤ４）。

【０２１２】

図２６のステップＤ４において乱数の値が奇数であった場合には、Ｒ２とＲ１との和の計算結果はＲ１に格納される。引き続いて、暗号化演算手段はラウンド関数中の排他的論理和（ビット毎の排他的論理和）２５４０および左ビット回転２５５０を行い、左ビット回転２５５０が終了した時点におけるＢの値をＲ３に格納する。

【０２１３】

さらに、Ｒ４にS_{2r+1}の値を格納し、Ｒ３とＲ４との和をＲ３に格納する。以上の操作により、ラウンド関数適用後のＡおよびＢの値がＲ１およびＲ３に格納される（ステップＤ５）。

【０２１４】

ステップＤ５の処理が終了したことによって１回のラウンド関数の処理が終了する。この時点で、現在までに暗号化処理装置が処理したラウンド関数の回数を表す変数ｒの値を調べ（ステップＤ７）、ｒの値がＲＣ５－３２／１２／１６が処理すべきラウンド関数の回数である１２と等しかった場合には、出力装置から暗号文を出力して処理を終了する（ステップＤ９）。それ以外の場合には、ｒに１を加え（ステップＤ８）、もう一度ラウンド関数を処理するためにステップＤ３に戻る。

【０２１５】

ステップＤ４において乱数が偶数であった場合には、Ｒ２とＲ１との和の計算結果はＲ２に格納される。

【０２１６】

引き続いて、暗号化処理装置はラウンド関数の排他的論理和（ビット毎の排他的論理和）２５４０および左ビット回転２５５０を行い、左ビット回転２５５０が終了した時点におけるＢの値をＲ３に格納する。

【０２１７】

さらに、Ｒ４にS_{2r+1}の値を格納し、Ｒ３とＲ４との和をＲ４に格納する。以上の操作により、ラウンド関数適用後のＡおよびＢの値がＲ２およびＲ４に格納

される（ステップＤ６）。

【０２１８】

次に、ステップＤ７の場合と同様に変数ｒの値が１２と等しいかどうかを調べ（ステップＤ１４）、等しい場合には出力装置から暗号文を出力して処理を終了する（ステップＤ１６）。それ以外の場合には、ｒに１を加え（ステップＤ１５）、もう一度ラウンド関数を処理するためにステップＤ１０に進む。

【０２１９】

ステップＤ１０では、ラウンド関数への入力ＡおよびＢの値がそれぞれＲ２およびＲ４に格納されている。暗号化処理装置は、図２５に示されるラウンド関数の排他的論理和２５１０および左ビット回転２５２０を実行し、さらに汎用レジスタＲ１にS_{2r}を格納する。この時点で、条件分岐制御手段が呼び出され、Ｒ１の保持するS_{2r}の値とＲ２の保持するＡの値との和（2^{32}を法とする和）２５３０をとった計算結果をＲ１およびＲ２のどちらに格納するかを乱数の値の偶奇に応じて変化させる（ステップＤ１０およびＤ１１）。

【０２２０】

図２６のステップＤ１１において乱数の値が奇数であった場合には、Ｒ２とＲ１との和の計算結果はＲ１に格納される。引き続いて、暗号化演算手段はラウンド関数中の排他的論理和２５４０および左ビット回転２５５０に対応する操作を行い、左ビット回転２５５０が終了した時点におけるＢの値をＲ４に格納する。さらにＲ３にS_{2r+1}の値を格納し、Ｒ３とＲ４との和をＲ３に格納する。以上の操作により、ラウンド関数適用後のＡおよびＢの値がＲ１およびＲ３に格納される（ステップＤ１２）。

【０２２１】

ステップＤ１２の処理が終了したことによって１回のラウンド関数の処理が終了する。この時点で、現在までに暗号化処理装置が処理したラウンド関数の回数を表す変数ｒの値を調べ（ステップＤ７）、ｒの値がＲＣ５－３２／１２／１６が処理すべきラウンド関数の回数である１２と等しかった場合には、出力装置から暗号文を出力して処理を終了する（ステップＤ９）。それ以外の場合には、ｒに１を加え（ステップＤ８）、もう一度ラウンド関数を処理するためにステップ

Ｄ３に戻る。

【０２２２】

ステップＤ１１において乱数が偶数であった場合には、Ｒ２とＲ１との和の計算結果はＲ２に格納される。引き続いて、暗号化処理装置はラウンド関数中の排他的論理和２５４０および左ビット回転２５５０に対応する操作を行い、左ビット回転２５５０が終了した時点におけるＢの値をＲ４に格納する。さらに、Ｒ３にS_{2r+1}の値を格納し、Ｒ３とＲ４との和をＲ４に格納する。以上の操作により、ラウンド関数適用後のＡおよびＢの値がＲ２およびＲ４に格納される（ステップＤ１３）。

【０２２３】

次に、ステップＤ７の場合と同様に、変数ｒの値が１２と等しいかどうかを調べ（ステップＤ１４）、等しい場合には出力装置から暗号文を出力して処理を終了する（ステップＤ１６）。それ以外の場合には、ｒに１を加え（ステップＤ１５）、もう一度ラウンド関数を処理するためにステップＤ１０に戻る。

【０２２４】

上記のアルゴリズムにより、乱数生成装置が出力した乱数の値に依存せずに、出力装置には入力平文を暗号化した結果が出力される。

【０２２５】

（３）　第３の実施例

図２７および図２８は、本発明の第３の実施例を説明するための図である。

【０２２６】

本実施例は、上述の第１５の実施の形態に係る暗号化・復号装置を、公開鍵暗号ＲＳＡに適用したものである。

【０２２７】

なお、ＲＳＡのアルゴリズムに関しては、上記の「Ｈａｎｄｂｏｏｋ　ｏｆ　Ａｐｐｌｉｅｄ　Ｃｒｙｐｔｏｇｒａｐｈｙ」のｐｐ．２８５－２９１に詳しく述べられている。

【０２２８】

ここでは、まず、ＲＳＡの動作の概要を説明する。

【０２２９】

ＲＳＡは５１２ビット程度の２つの素数ｐ，ｑの積ｎと、ｌｃｍ（ｐ－１，ｑ－１）（ただし、ｌｃｍ（ａ，ｂ）はａとｂとの最小公倍数を表す）と互いに素である数ｅの組（ｎ，ｅ）とを公開鍵として持ち、法ｌｃｍ（ｐ－１，ｑ－１）の下でｅｄ＝１となるようなｄを秘密鍵として持つ。

【０２３０】

ＲＳＡの暗号化は、次のように行われる。

【０２３１】

Ｍを暗号化したい平文とすると、Ｍを暗号化した暗号文Ｃは次式に従って計算される。

【０２３２】

$C=M^{e} \mod n$

【０２３３】

また、暗号文Ｃから平文Ｍを復号する計算は、次式で表される。

【０２３４】

$M=C^{d} \mod n$

【０２３５】

ＲＳＡでは、暗号化や復号を高速に行うために、高速な冪乗剰余演算アルゴリズムが必要となる。ここで冪乗剰余演算アルゴリズムとは、ｇ，ｅ，ｎを入力として$g^{e} \mod n$を出力するアルゴリズムを指す。

【０２３６】

ＲＳＡの実装では、高速な冪乗剰余演算アルゴリズムとして図２７の流れ図で示されるアルゴリズムまたはその改良アルゴリズムを用いることが標準的である。ここでは、図２７の流れ図を基に、高速冪乗剰余演算アルゴリズムの動作の流れを説明する。

【０２３７】

冪乗剰余アルゴリズムでは、まず初めに、ｇ，ｅ，ｎが入力される（図２７のステップＥ１）。

【０２３８】

続いて、変数ＡおよびＳに初期値として１およびｇをそれぞれ格納する（ステップＥ２）。

【０２３９】

続いて、ｅが０であるかどうかを判定し（ステップＥ３）、０の場合にはＡを出力して処理を終了し、そうでない場合にはｅの偶奇を調べ、ｅが奇数であった場合にはＡとＳとの積を計算し、その結果を新たに再びＡに格納する（ステップＥ４およびＥ５）。

【０２４０】

次に、ｅの値を２で割ることにより、ｅの１ビット右シフトを行う（ステップＥ６）。

【０２４１】

この段階で再びｅが０であるかどうかを判定し（ステップＥ７）、０である場合にはＡを出力して処理を終了し、そうでない場合にはＳを二乗して（ステップＥ８）、ステップＥ３に戻る。

【０２４２】

ｅの二進数表現を（b_1，b_2，…，b_t）とすると（ただし、b_1が最上位ビット、b_tが最下位ビット）、図２７の流れ図においてステップＥ７をｉ回通過した時点でのＡの値は、二進数表現が（b_1，b_2，…，b_i）となるような数ｅｉに対して$g^{ei} \bmod n$となっている。

【０２４３】

アルゴリズムの構成法により、図２７で示されるアルゴリズムではｅのビット長ｔに対してアルゴリズム終了時までにステップＥ７を通過する回数は必ずｔ回となるので、アルゴリズム終了時のＡの値は$g^{e} \bmod n$となり冪乗剰余演算が計算されていることが分かる。

【０２４４】

しかし、上記のようなアルゴリズムを用いて冪乗剰余演算を実現する場合には、次のような問題が生じる。図２７のステップＥ４をｉ回通過した後にステップＥ５が実行される必要十分条件は、ｅの右からｉビット目が１であることとなる。この時、上記のアルゴリズムを実装した装置の実行中に当該装置が消費する電

力を測定することにより、当該装置内で実行されている命令の特定が可能であるとすると、ＲＳＡ暗号文の復号時における当該装置の消費電力を測定することによりＲＳＡの秘密鍵ｄを特定することが可能になってしまう。

【０２４５】

次に、図２７の流れ図および図２８を参照して本実施例を詳細に説明する。

【０２４６】

本実施例の暗号化・復号装置における暗号化・復号処理装置２８２０は、暗号化・復号演算手段２８２１と、乱数依存性決定手段２８２２と、遅延制御手段２８２３とを備えており、次のように動作する。

【０２４７】

暗号化・復号演算手段２８２１は、２つの相異なる数ａ，ｂと法ｎとを入力とし、ａ・ｂｍｏｄｎを計算する乗算器２８２１１と、１つの数ａと法ｎとを入力とし、a^2 ｍｏｄｎを計算する二乗演算器２８２１２とを備えている。

【０２４８】

暗号化・復号演算手段２８２１は、暗号化と復号との２つの機能を有しており、暗号化を行う場合には入力装置２８１０から通信相手の公開鍵ｅ，n_1 と送信したい平文Ｍとを入力し、図２７の流れ図と同様な動作を行うことによって、暗号文M^e ｍｏｄn_1 を計算し、その計算結果を出力装置２８５０より出力する。また、復号を行う場合には、入力装置２８１０から本人の秘密鍵ｄと本人の公開鍵n_2 および受信した暗号文Ｃとを入力し、図２７の流れ図と同様な動作を行うことによって、平文C^d ｍｏｄn_2 を計算し、その計算結果を出力装置２８５０より出力する。

【０２４９】

図２８中の暗号化・復号演算手段２８２１の動作が図２７の流れ図と異なる点は、図２８中の暗号化・復号演算手段２８２１は、図２７のステップＥ８からステップＥ３に戻る時点で乱数依存性決定手段２８２２によって遅延時間決定要求が遅延制御手段２８２３に出力される点にある。

【０２５０】

遅延制御手段２８２３は、暗号化演算手段２８２１と同様に、乗算器２８２３

１と、二乗演算器２８２３２とを備えており、乱数依存性決定手段２８２２より遅延時間決定要求が出されると、乱数生成装置２８４０に対して乱数要求信号を２度送り、２つの乱数ｒ１，ｒ２を得る。

【０２５１】

ｒ１とｒ２とを受け取った遅延制御手段２８２３は、ｒ１の最下位ビットが０であるか否かを判定し、０であった場合には遅延挿入のために、二乗演算器２８２３２を用いてｒ２の二乗の計算を行い、再び暗号化・復号演算手段２８２１に処理を移す。一方、ｒ１の最下位ビットが１であった場合には、遅延挿入のために、遅延制御手段２８２３は、乗算器２８２３１を用いてｒ１とｒ２との積を計算した後に、二乗演算器２８２３２を用いて乗算器２８２３１の計算結果であるｒ１・ｒ２の二乗を計算し、再び暗号化・復号演算手段２８２１に処理を移す。

【０２５２】

【発明の効果】

以上説明したように、本発明の暗号化装置，復号装置，および暗号化・復号装置によると、データの暗号化や復号を行う際に当該装置の消費電力を測定することによって暗号化鍵や復号鍵等の秘密情報を得る暗号解析法（電力解析や電力差分解析等の消費電力の測定による暗号解析法）の適用が困難になるという効果が生じる。

【０２５３】

以上のような効果が生じる理由を、以下に述べる。

【０２５４】

電力解析や電力差分解析等の消費電力の測定による暗号解析が成功するためには、第１に暗号化装置や復号装置がデータの暗号化や復号を行っている際に消費する電力と当該装置内で行われている暗号化操作や復号操作との間に密接な関連があること、第２に暗号化装置や復号装置が特定の暗号化操作や復号操作を行っている時刻が容易に検知できること、の２点が必要条件となる。

【０２５５】

本発明では、中間データ制御手段によって暗号化や復号を行う際に必要となる

中間データが乱数に依存して変化したまま暗号装置や復号装置内で暗号化操作や復号操作が行われるため、当該装置が消費した電力の変化が実際の暗号化操作や復号操作によって生じたものであるのか、乱数の影響によって生じたものであるのかの判断が困難になっている。したがって、暗号化装置や復号装置の消費電力と当該装置内で行われている暗号化操作や復号操作との間の関連が検知しづらくなるため、電力解析や電力差分解析が成功するための第１の必要条件が成立しなくなる。

【０２５６】

さらに、本発明では、条件分岐制御手段によって、順序を入れ替えることが可能であるような操作の順序（実行順序）の決定や、どの操作を実行しても暗号化や復号の結果が変化しないような複数の操作の選択肢の中から実際に実行される操作を選択することを、乱数に依存して行っている。また、遅延制御手段によって、暗号化や復号の操作の途中で、適宜乱数に依存した時間の遅延が挿入される。それらのために、特定の暗号化や復号の操作が実行される時刻が、乱数によって変化することになる。したがって、電力解析や電力差分解析が成功するための第２の必要条件が成立しなくなる。

【０２５７】

以上により、電力解析や電力差分解析の成功に必要な２つの条件が成立しなくなるため、暗号化装置や復号装置の消費電力を測定することで秘密情報を得るという暗号解析法が困難になる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図２】

図１に示す暗号化装置の処理を示す流れ図である。

【図３】

本発明の第２の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図４】

図３に示す暗号化装置の処理を示す流れ図である。

【図５】

本発明の第３の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図６】

図５に示す暗号化装置の処理を示す流れ図である。

【図７】

本発明の第４の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図８】

本発明の第５の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図９】

本発明の第６の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図１０】

本発明の第７の実施の形態に係る復号装置の構成を示すブロック図である。

【図１１】

本発明の第８の実施の形態に係る復号装置の構成を示すブロック図である。

【図１２】

本発明の第９の実施の形態に係る復号装置の構成を示すブロック図である。

【図１３】

本発明の第１０の実施の形態に係る復号装置の構成を示すブロック図である。

【図１４】

本発明の第１１の実施の形態に係る復号装置の構成を示すブロック図である。

【図１５】

本発明の第１２の実施の形態に係る復号装置の構成を示すブロック図である。

【図１６】

本発明の第１３の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図１７】

本発明の第１４の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図１８】

本発明の第１５の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図１９】

本発明の第１６の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図２０】

本発明の第１７の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図２１】

本発明の第１８の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図２２】

本発明の第１の実施例を説明するための図（ＤＥＳの構成を示すブロック図）である。

【図２３】

本発明の第１の実施例を説明するための図（当該実施例の構成を示すブロック図）である。

【図２４】

本発明の第２の実施例を説明するための図（ＲＣ５－３２/１２/１６の構成を示すブロック図）である。

【図２５】

本発明の第２の実施例を説明するための図（ＲＣ５－３２/１２/１６のラウンド関数の構成を示すブロック図）である。

【図２６】

本発明の第２の実施例を説明するための図（当該実施例の動作を示す流れ図）である。

【図２７】

本発明の第３の実施例を説明するための図（高速冪乗剰余演算の動作を示す流れ図）である。

【図２８】

本発明の第３の実施例を説明するための図（当該実施例の構成を示すブロック図）である。

【符号の説明】

１１０，３１０，５１０，１０１０，１１１０，１２１０，１６１０，１７１０，１８１０，２８１０　入力装置

１２０，３２０，５２０　暗号化処理装置

１２１，３２１，５２１　暗号化演算手段

１２２，３２２，５２２，１０２２，１１２２，１２２２，１６２２，１７２２，１８２２，２８２２　乱数依存性決定手段

１２３，１０２３，１６２３　中間データ制御手段

１３０，３３０，５３０，１０３０，１１３０，１２３０，１６３０，１７３０，１８３０，２８３０　記憶装置

１３１，３３１，５３１，１０３１，１１３１，１２３１，１６３１，１７３１，１８３１，２８３１　中間データ記憶部

１４０，３４０，５４０，１０４０，１１４０，１２４０，１６４０，１７４０，１８４０，２８４０　乱数生成装置

１５０，３５０，５５０，１０５０，１１５０，１２５０，１６５０，１７５０，１８５０，２８５０　出力装置

３２３，１１２３，１７２３　条件分岐制御手段

５２３，１２２３，１８２３，２８２３　遅延制御手段

７００，８００，９００，１３００，１４００，１５００，１９００，２０００，２１００　記録媒体

１０２０，１１２０，１２２０　復号処理装置

１０２１，１１２１，１２２１　復号演算手段

１６２０，１７２０，１８２０，２８２０　暗号化・復号処理装置

１６２１，１７２１，１８２１，２８２１　暗号化・復号演算手段

２２１０　鍵スケジューリング部

２２２０，２４３０　データ処理部

２３１０，２３２０，２３３０，２３４０，２３５０，２３６０，２３７０，２３８０　乱数依存性付与部分

２４１０　平文

２４２０　暗号化鍵

２４３１，２４３２，２５３０，２５６０　2^{32}を法とする和

２４４０　拡大鍵生成部

２４５０　暗号文

２５１０，２５４０　ビット毎の排他的論理和

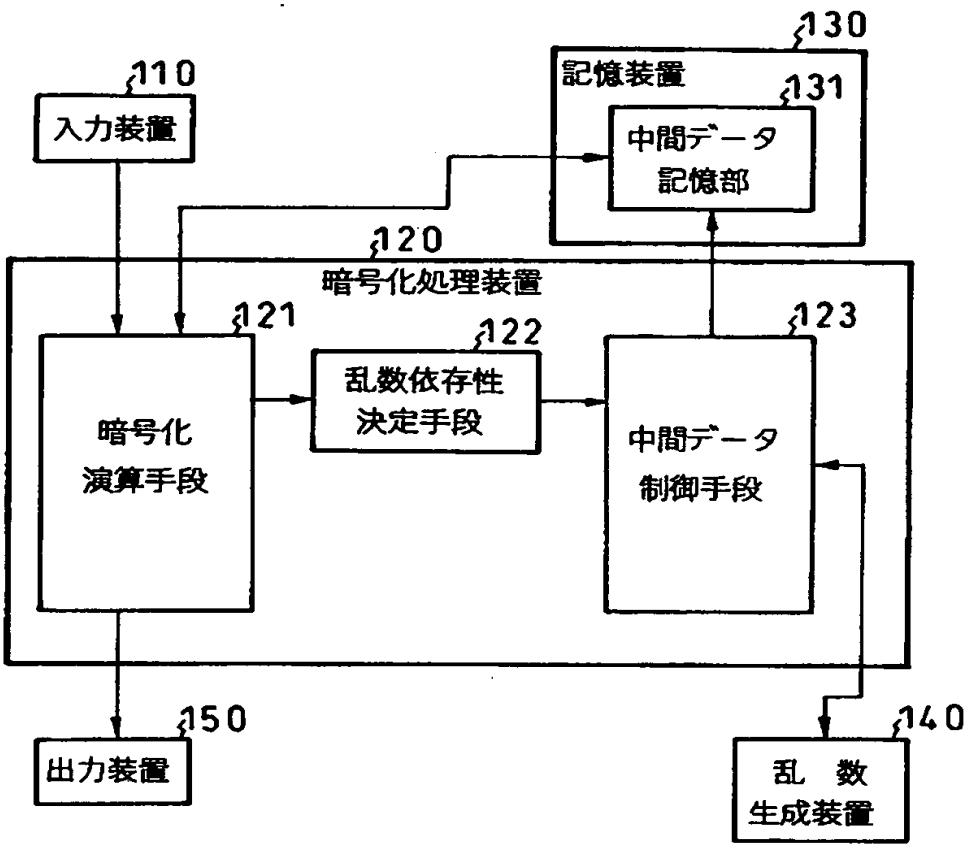
２５２０，２５５０　左ビット回転

２８２１１，２８２３１　乗算器

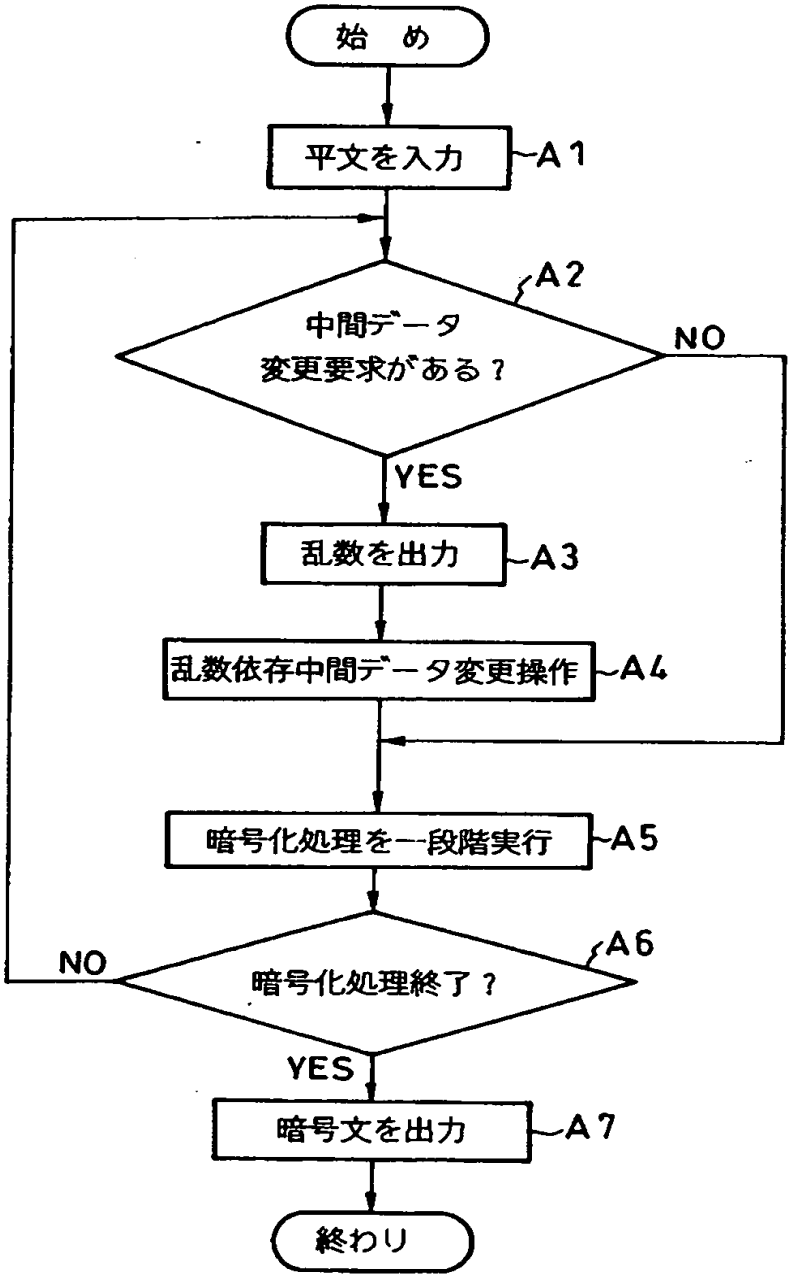
２８２１２，２８２３２　二乗演算器

【書類名】　図面

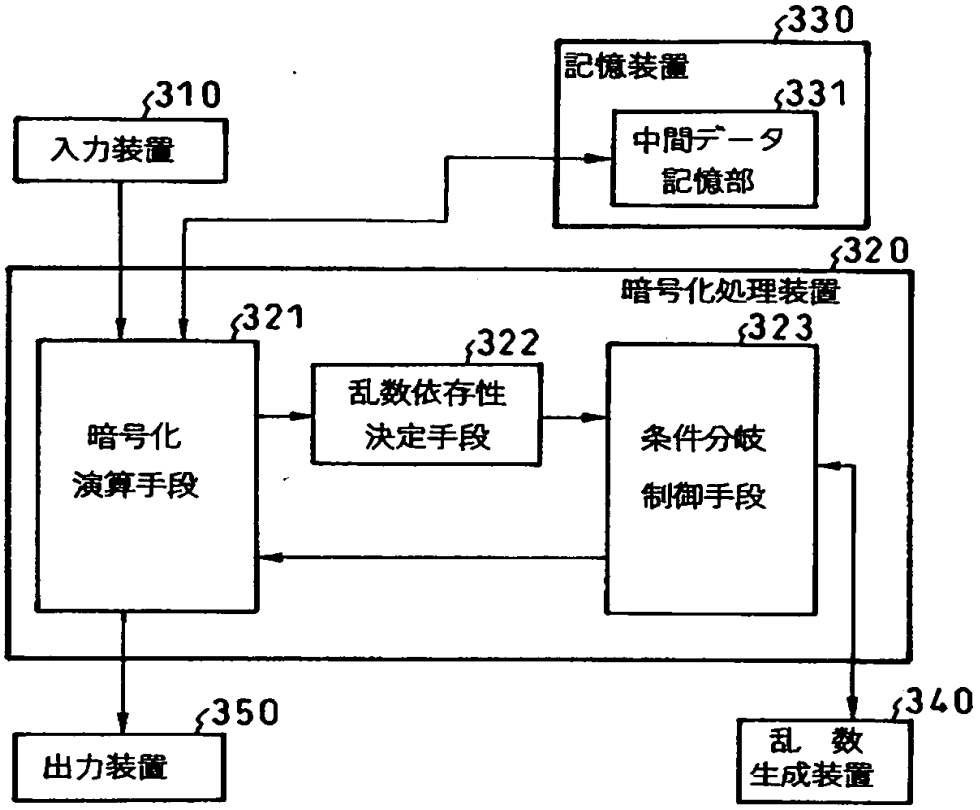
【図１】


130
記憶装置
131
中間データ
記憶部
110
入力装置
120
暗号化処理装置
121
暗号化
演算手段
122
乱数依存性
決定手段
123
中間データ
制御手段
150
出力装置
140
乱　数
生成装置

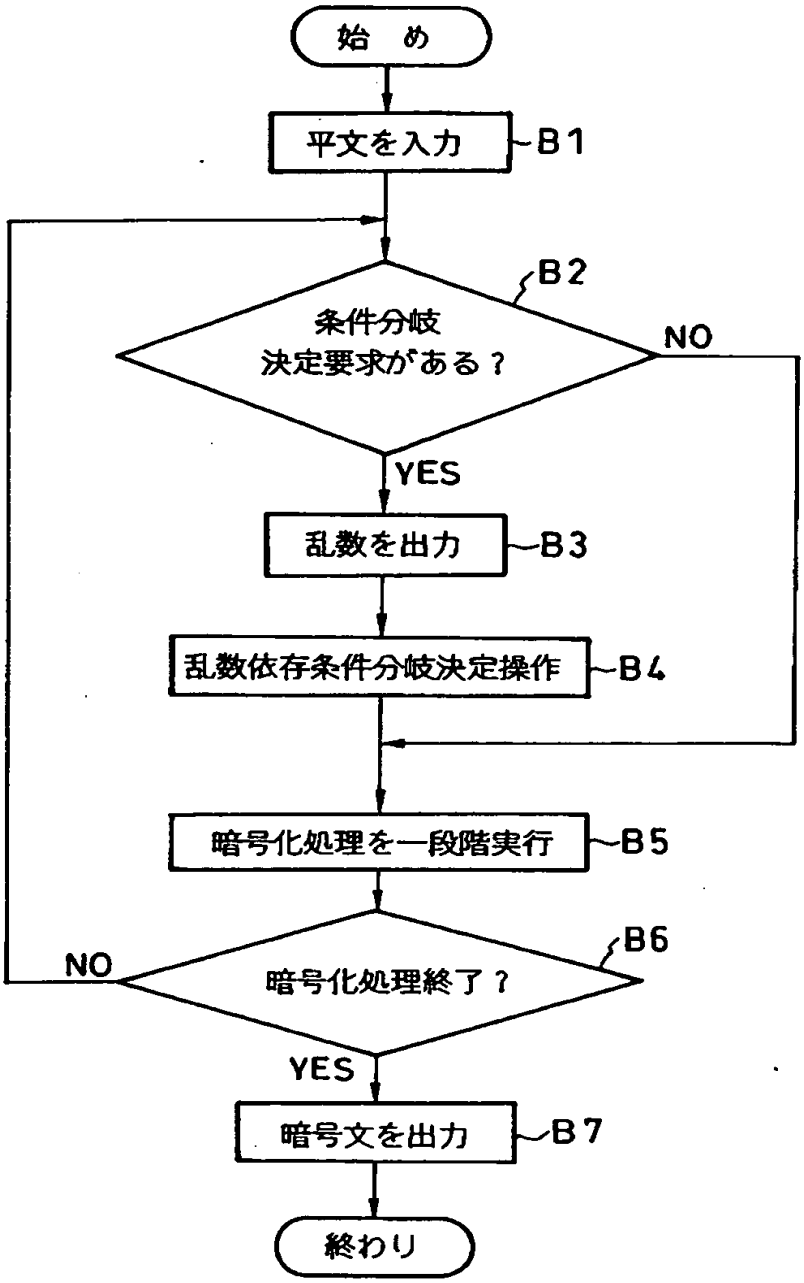
【図２】


始　め
平文を入力
A1
A2
中間データ
変更要求がある？
NO
YES
乱数を出力
A3
乱数依存中間データ変更操作
A4
暗号化処理を一段階実行
A5
A6
NO
暗号化処理終了？
YES
暗号文を出力
A7
終わり

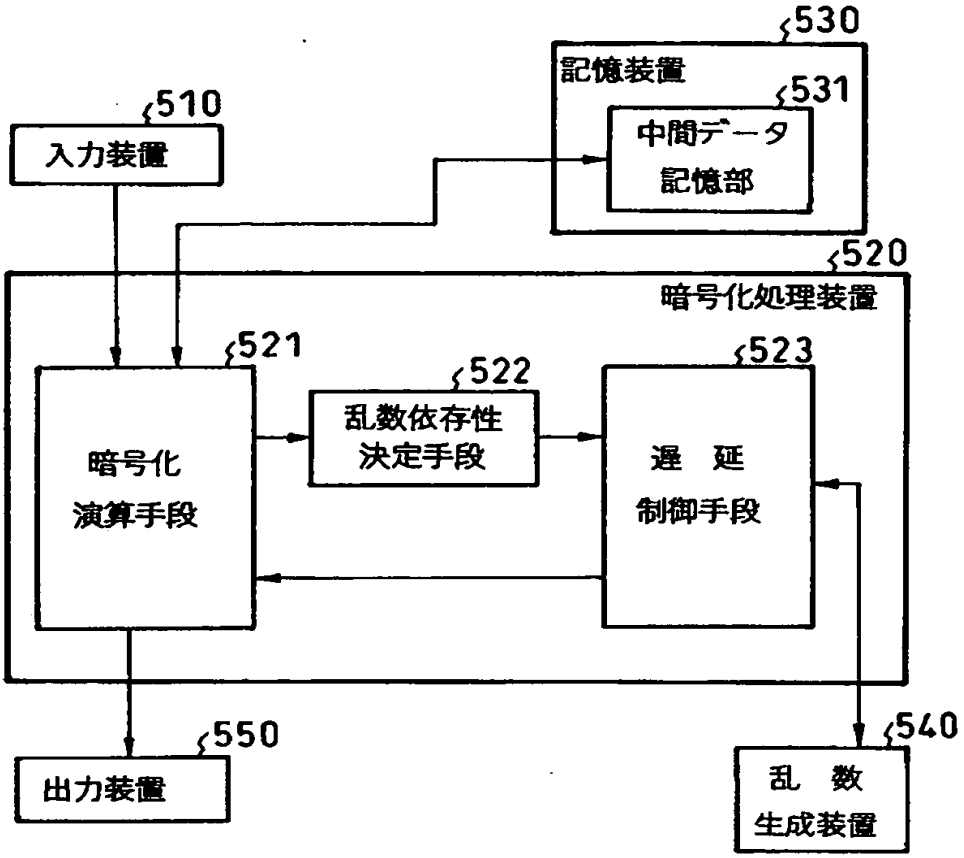
【図３】


330
記憶装置
331
中間データ
記憶部
310
入力装置
320
暗号化処理装置
321
暗号化
演算手段
322
乱数依存性
決定手段
323
条件分岐
制御手段
350
出力装置
340
乱　数
生成装置

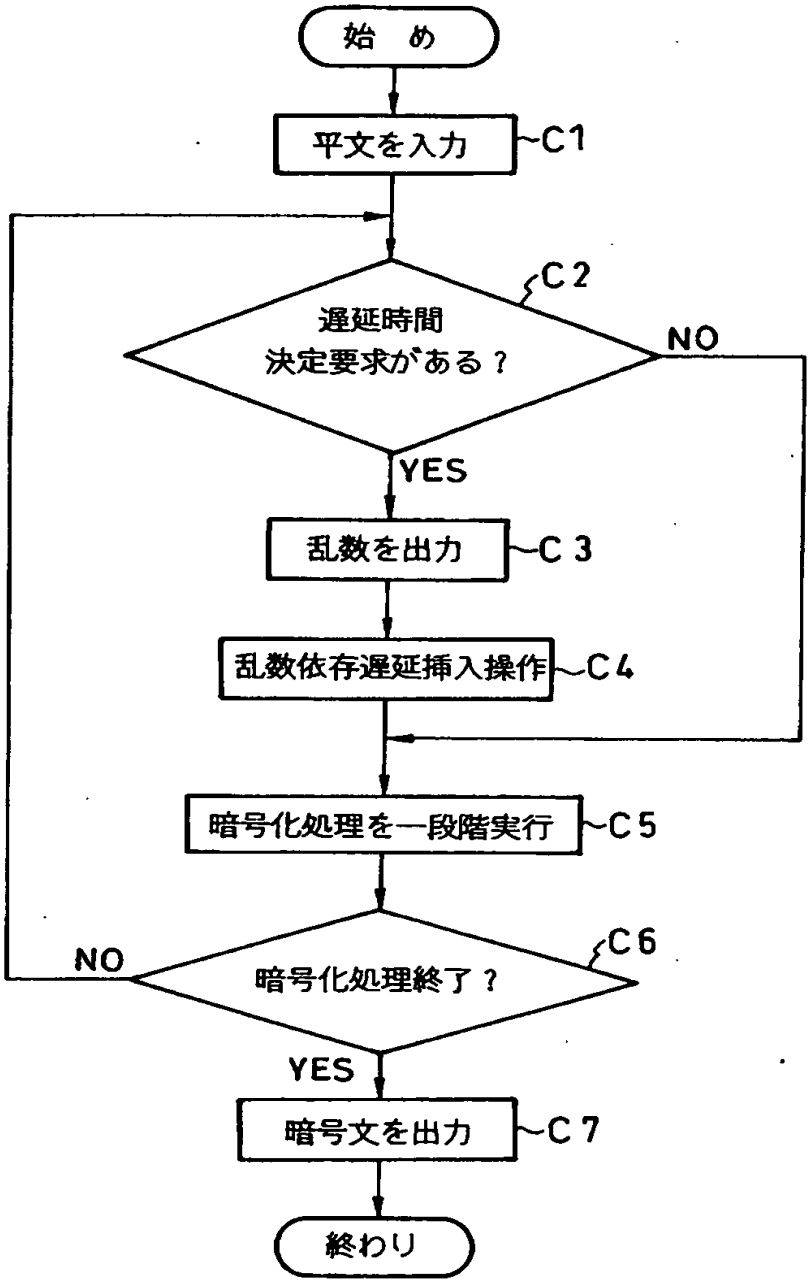
【図４】


始　め
平文を入力
B1
B2
条件分岐
決定要求がある？
NO
YES
乱数を出力
B3
乱数依存条件分岐決定操作
B4
暗号化処理を一段階実行
B5
B6
NO
暗号化処理終了？
YES
暗号文を出力
B7
終わり

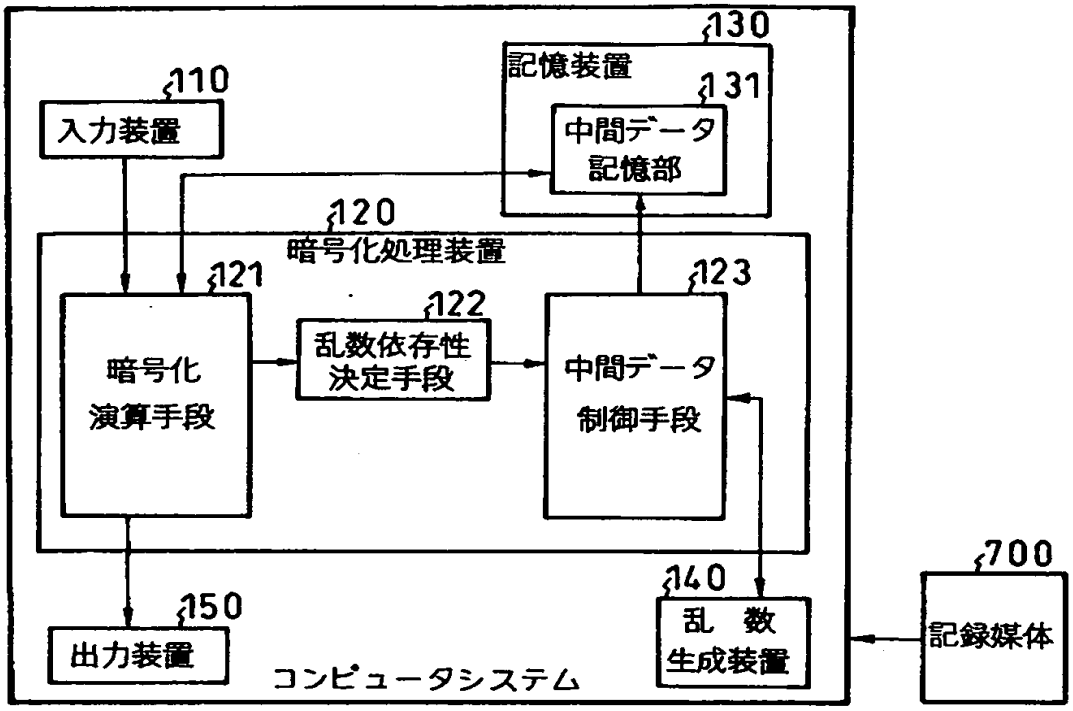
【図５】


530
記憶装置
531
中間データ
記憶部
510
入力装置
520
暗号化処理装置
521
暗号化
演算手段
522
乱数依存性
決定手段
523
遅　延
制御手段
550
出力装置
540
乱　数
生成装置

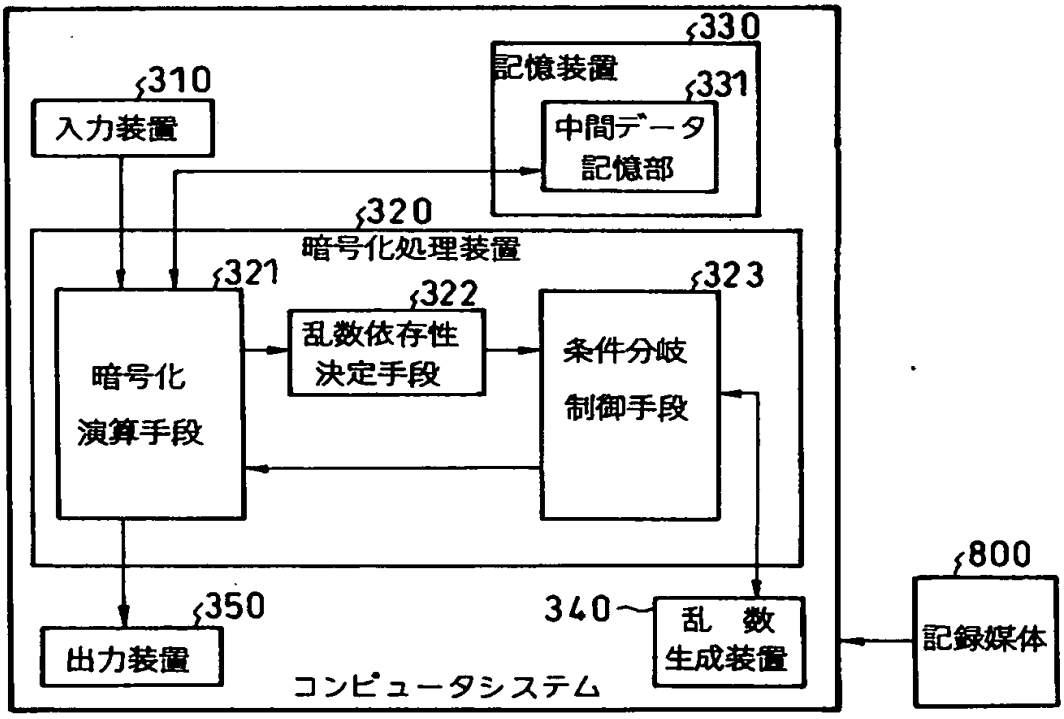
【図６】


始　め
平文を入力
C1
C2
遅延時間
決定要求がある？
NO
YES
乱数を出力
C3
乱数依存遅延挿入操作
C4
暗号化処理を一段階実行
C5
C6
NO
暗号化処理終了？
YES
暗号文を出力
C7
終わり

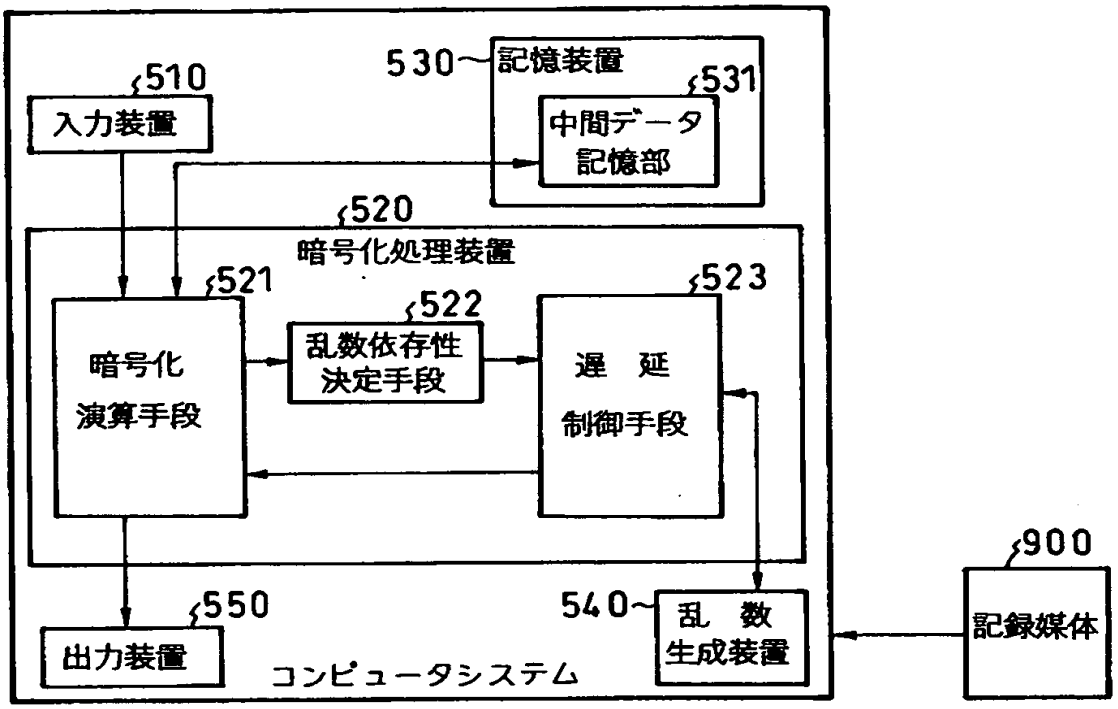
【図７】


130
記憶装置
131
中間データ記憶部
110
入力装置
120
暗号化処理装置
121
暗号化演算手段
122
乱数依存性決定手段
123
中間データ制御手段
700
140
乱　数生成装置
記録媒体
150
出力装置
コンピュータシステム

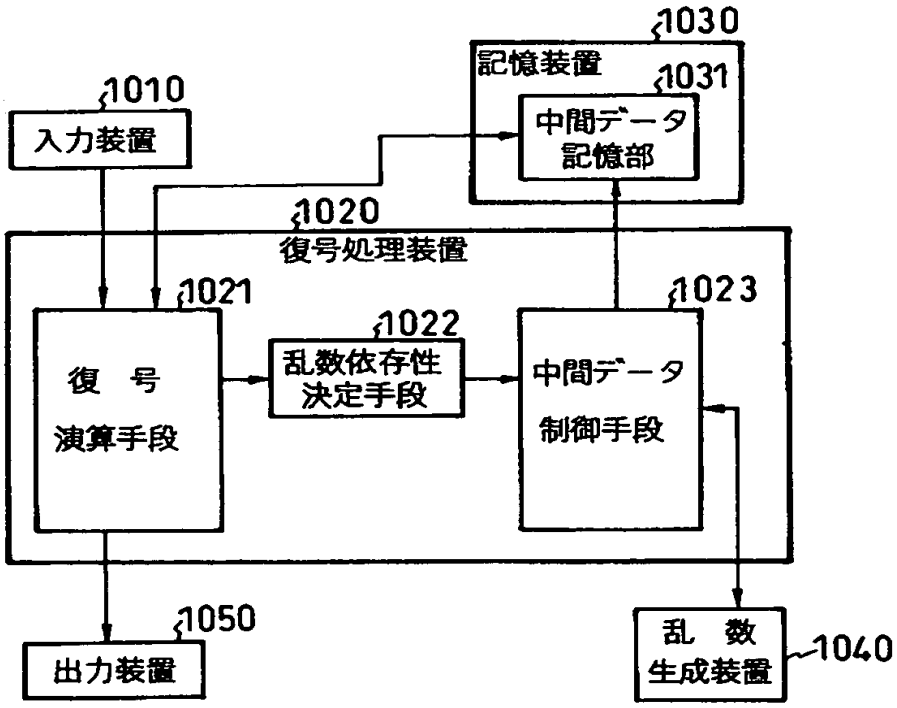
【図８】


330
記憶装置
331
中間データ記憶部
310
入力装置
320
暗号化処理装置
321
暗号化演算手段
322
乱数依存性決定手段
323
条件分岐制御手段
800
350
出力装置
340
乱　数生成装置
記録媒体
コンピュータシステム

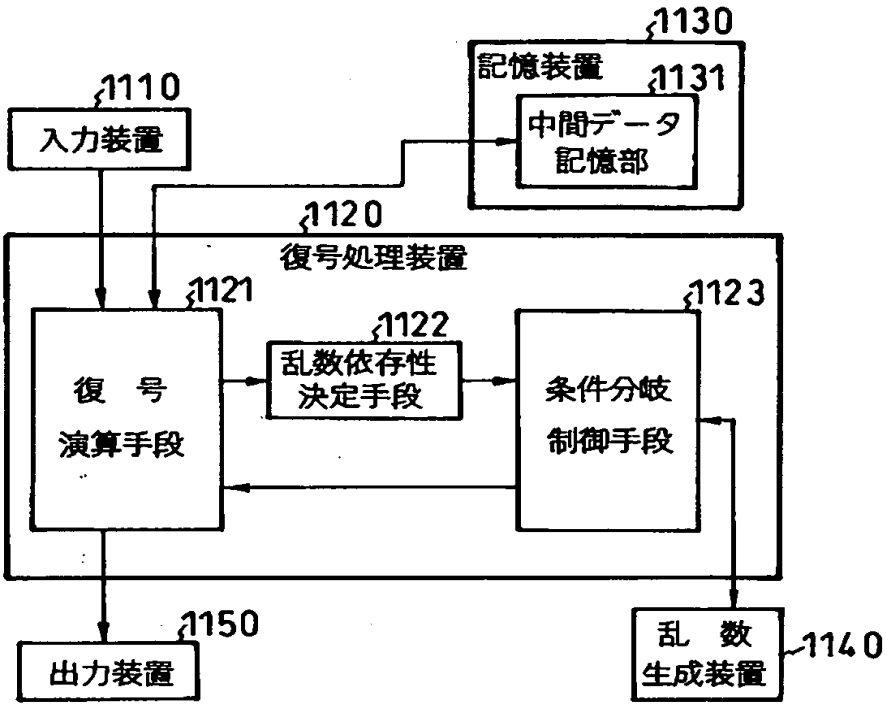
【図９】


510
入力装置
530
記憶装置
531
中間データ記憶部
520
暗号化処理装置
521
暗号化演算手段
522
乱数依存性決定手段
523
遅延制御手段
900
記録媒体
550
出力装置
540
乱数生成装置
コンピュータシステム

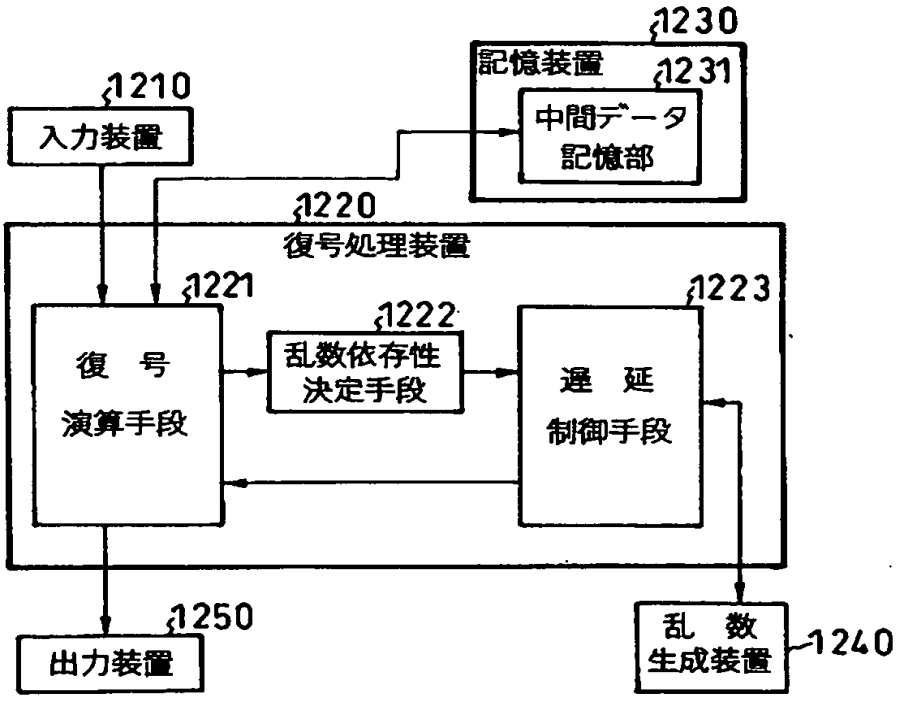
【図１０】


1030
記憶装置
1031
中間データ記憶部
1010
入力装置
1020
復号処理装置
1021
復号演算手段
1022
乱数依存性決定手段
1023
中間データ制御手段
1050
出力装置
乱数生成装置
1040

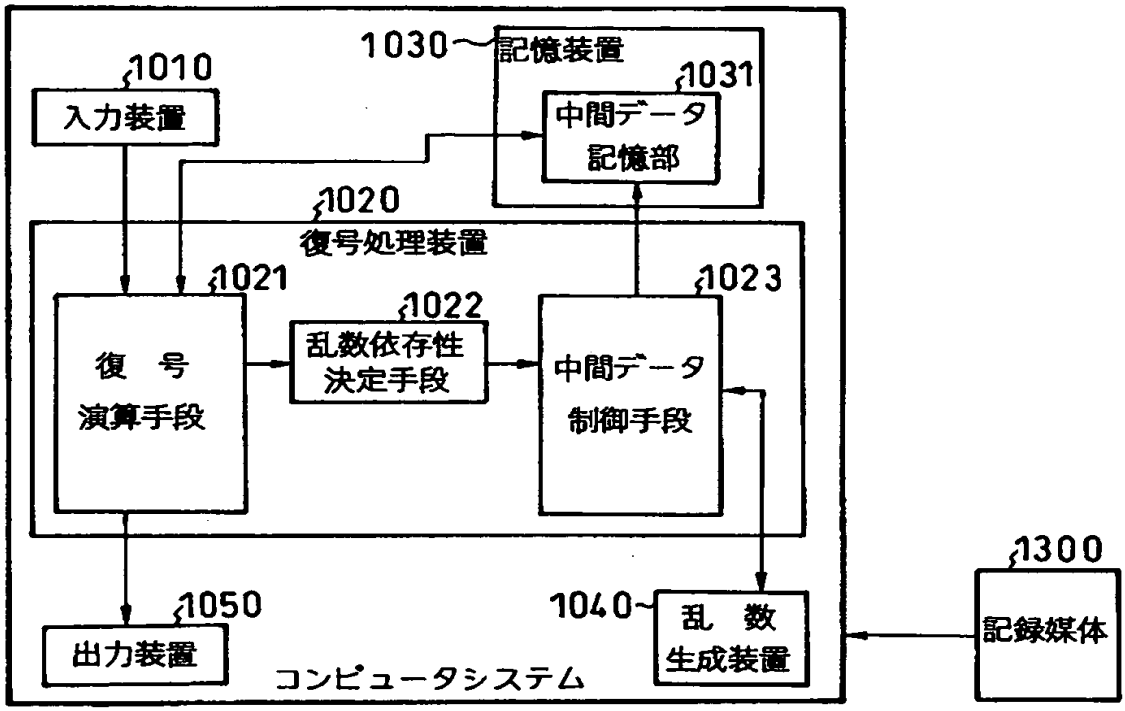
【図１１】


1130
記憶装置
1131
中間データ記憶部
1110
入力装置
1120
復号処理装置
1121
復　号
演算手段
1122
乱数依存性
決定手段
1123
条件分岐
制御手段
1150
出力装置
乱　数
生成装置
1140

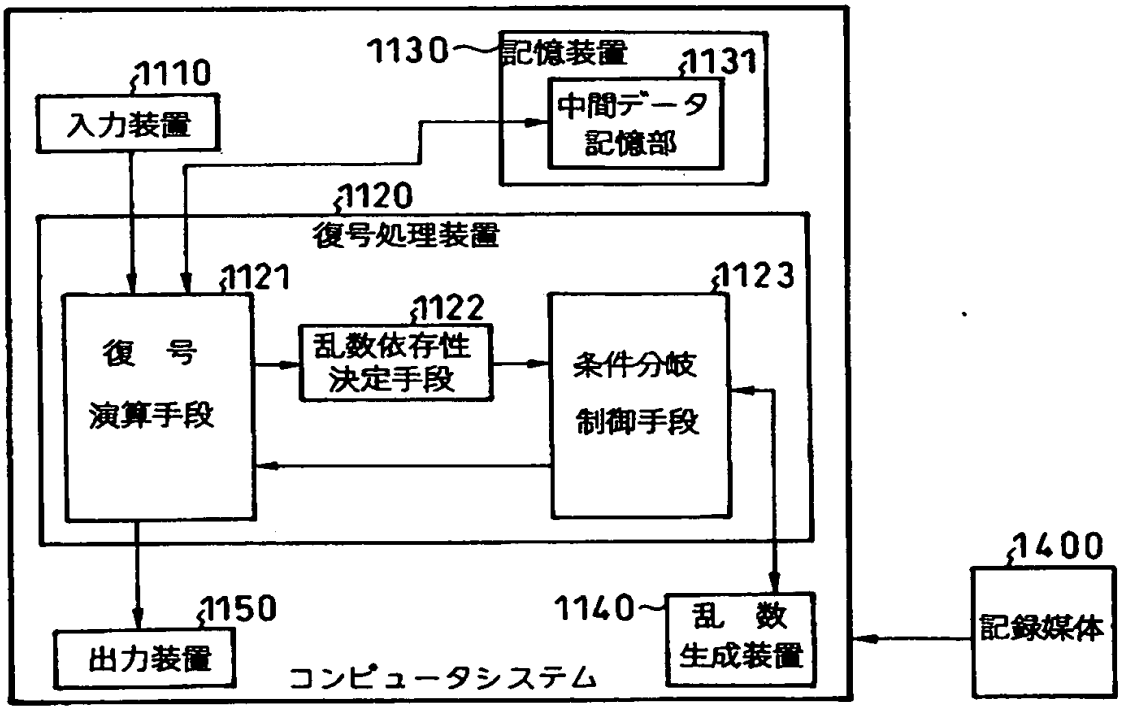
【図１２】


1230
記憶装置
1231
中間データ記憶部
1210
入力装置
1220
復号処理装置
1221
復　号
演算手段
1222
乱数依存性
決定手段
1223
遅　延
制御手段
1250
出力装置
乱　数
生成装置
1240

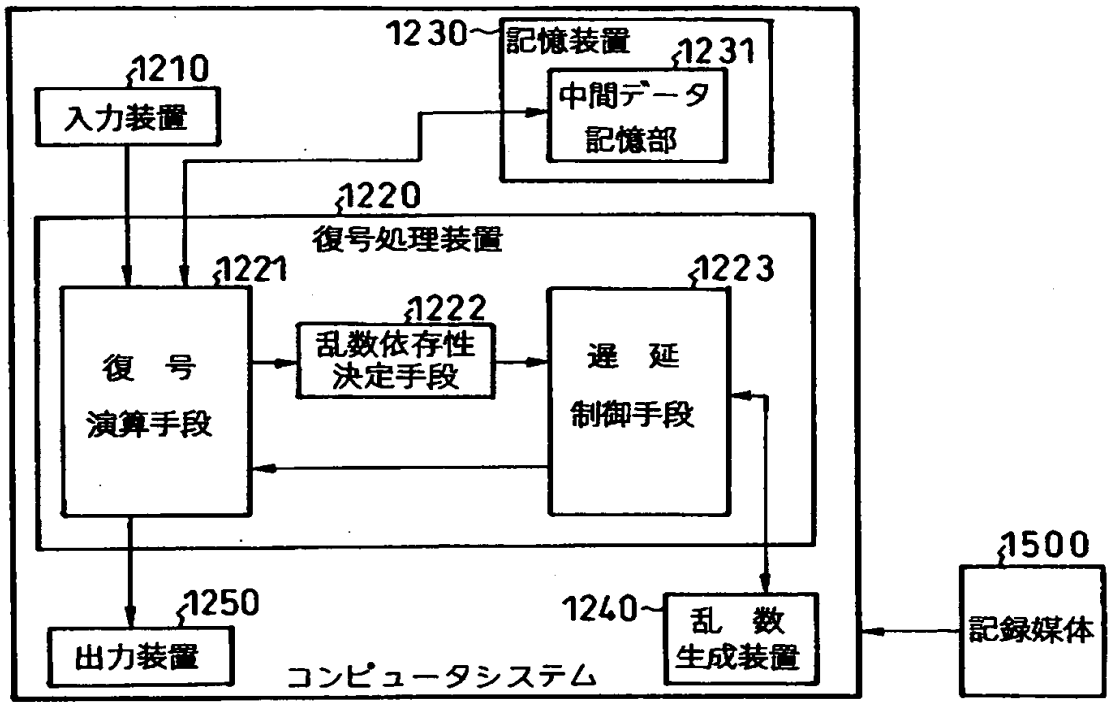
【図１３】


1010
入力装置
1030
記憶装置
1031
中間データ記憶部
1020
復号処理装置
1021
復　号演算手段
1022
乱数依存性決定手段
1023
中間データ制御手段
1050
出力装置
1040
乱　数生成装置
コンピュータシステム
1300
記録媒体

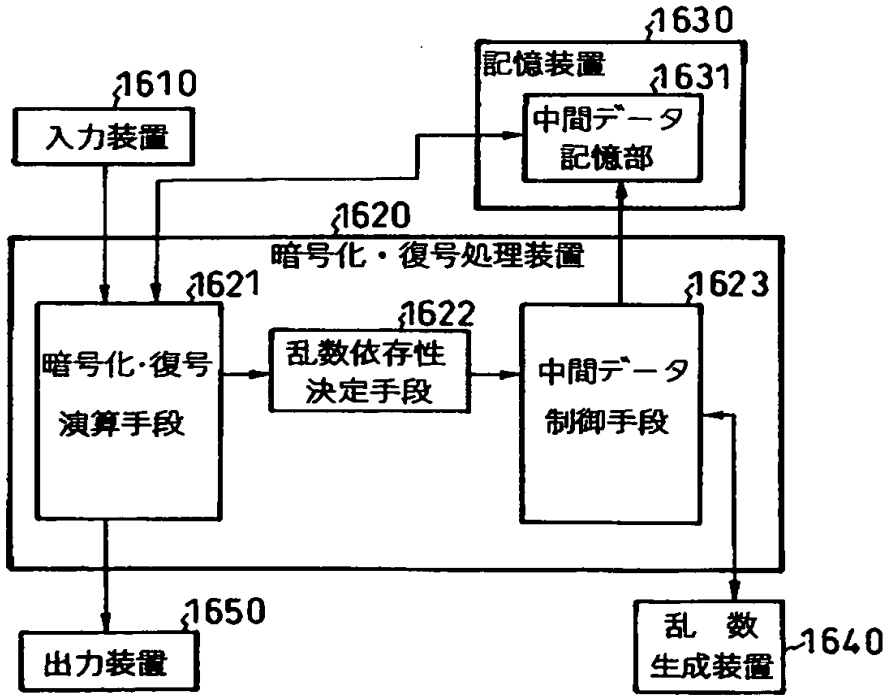
【図１４】


1110
入力装置
1130
記憶装置
1131
中間データ記憶部
1120
復号処理装置
1121
復　号演算手段
1122
乱数依存性決定手段
1123
条件分岐制御手段
1150
出力装置
1140
乱　数生成装置
コンピュータシステム
1400
記録媒体

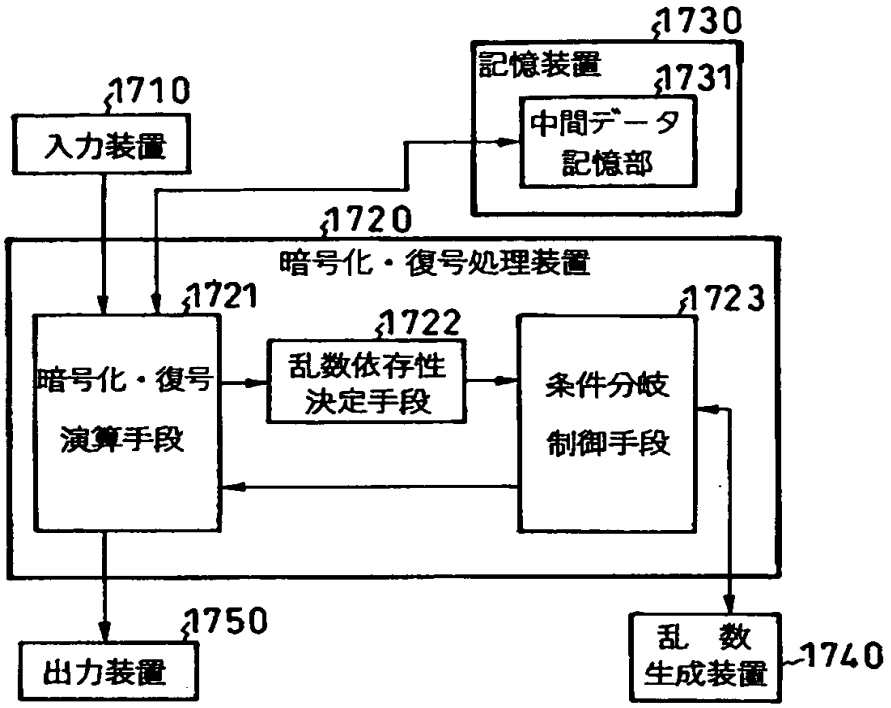
【図１５】


1230
記憶装置
1231
中間データ記憶部
1210
入力装置
1220
復号処理装置
1221
復　号演算手段
1222
乱数依存性決定手段
1223
遅　延制御手段
1500
1250
出力装置
1240
乱　数生成装置
記録媒体
コンピュータシステム

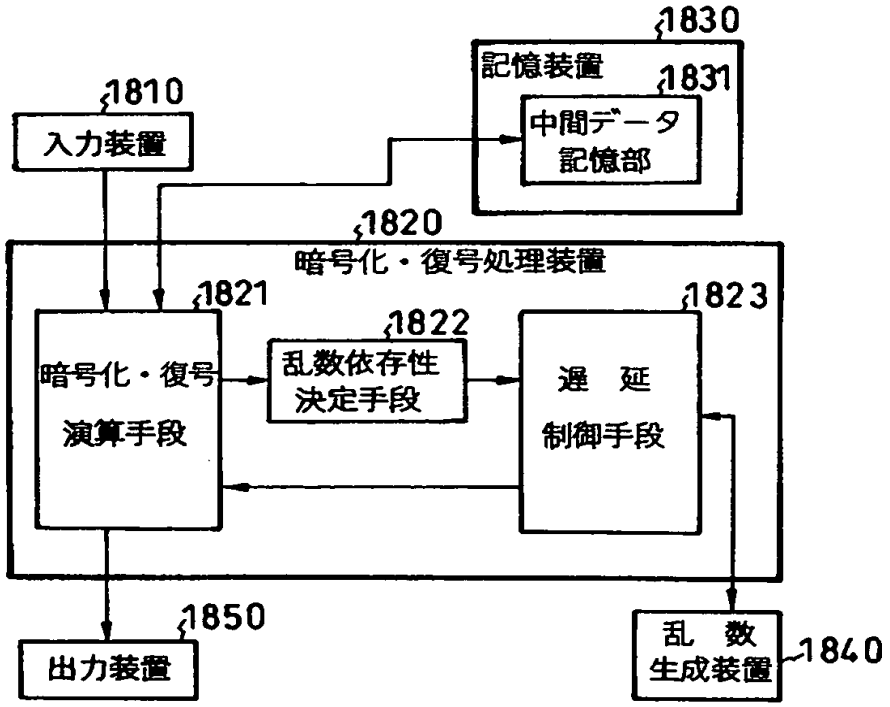
【図１６】


1630
記憶装置
1631
中間データ記憶部
1610
入力装置
1620
暗号化・復号処理装置
1621
暗号化･復号演算手段
1622
乱数依存性決定手段
1623
中間データ制御手段
1650
出力装置
乱　数生成装置
1640

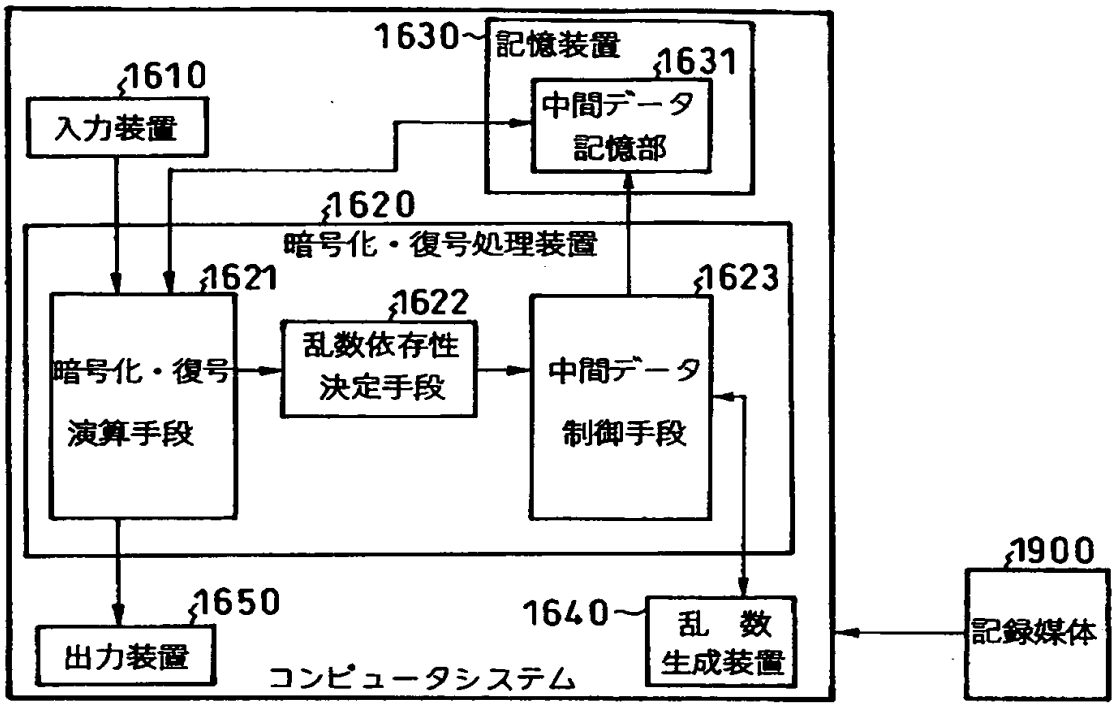
【図１７】


1730
記憶装置
1731
中間データ記憶部
1710
入力装置
1720
暗号化・復号処理装置
1721
暗号化・復号演算手段
1722
乱数依存性決定手段
1723
条件分岐制御手段
1750
出力装置
乱数生成装置
1740

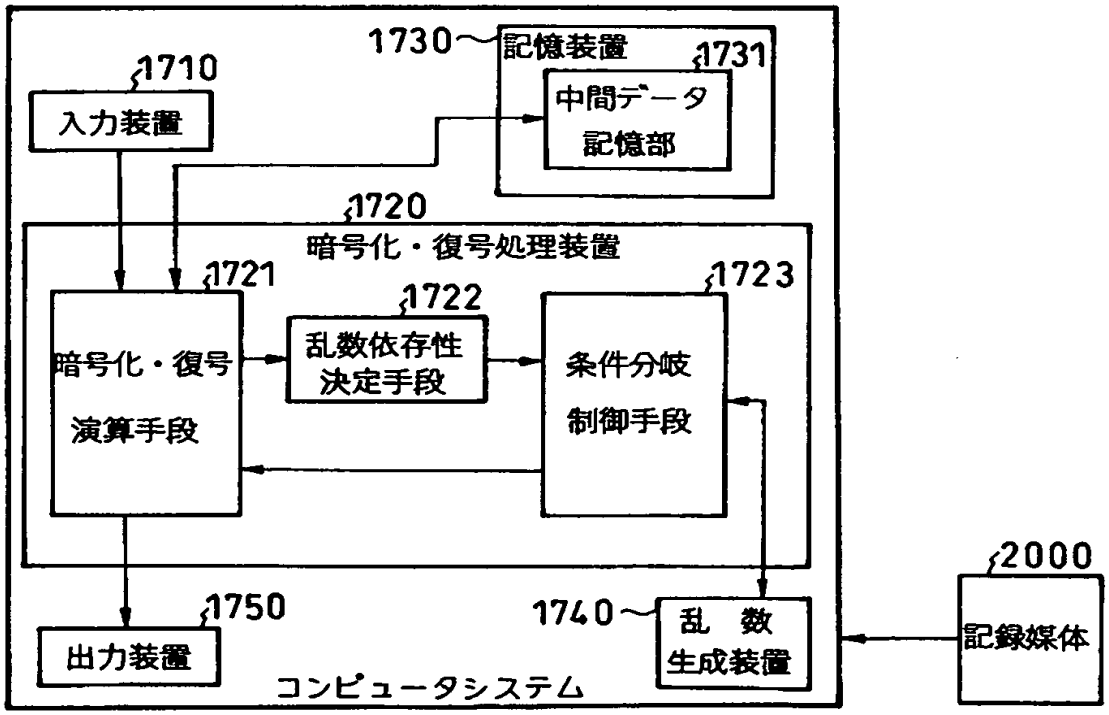
【図１８】


1830
記憶装置
1831
中間データ記憶部
1810
入力装置
1820
暗号化・復号処理装置
1821
暗号化・復号演算手段
1822
乱数依存性決定手段
1823
遅延制御手段
1850
出力装置
乱数生成装置
1840

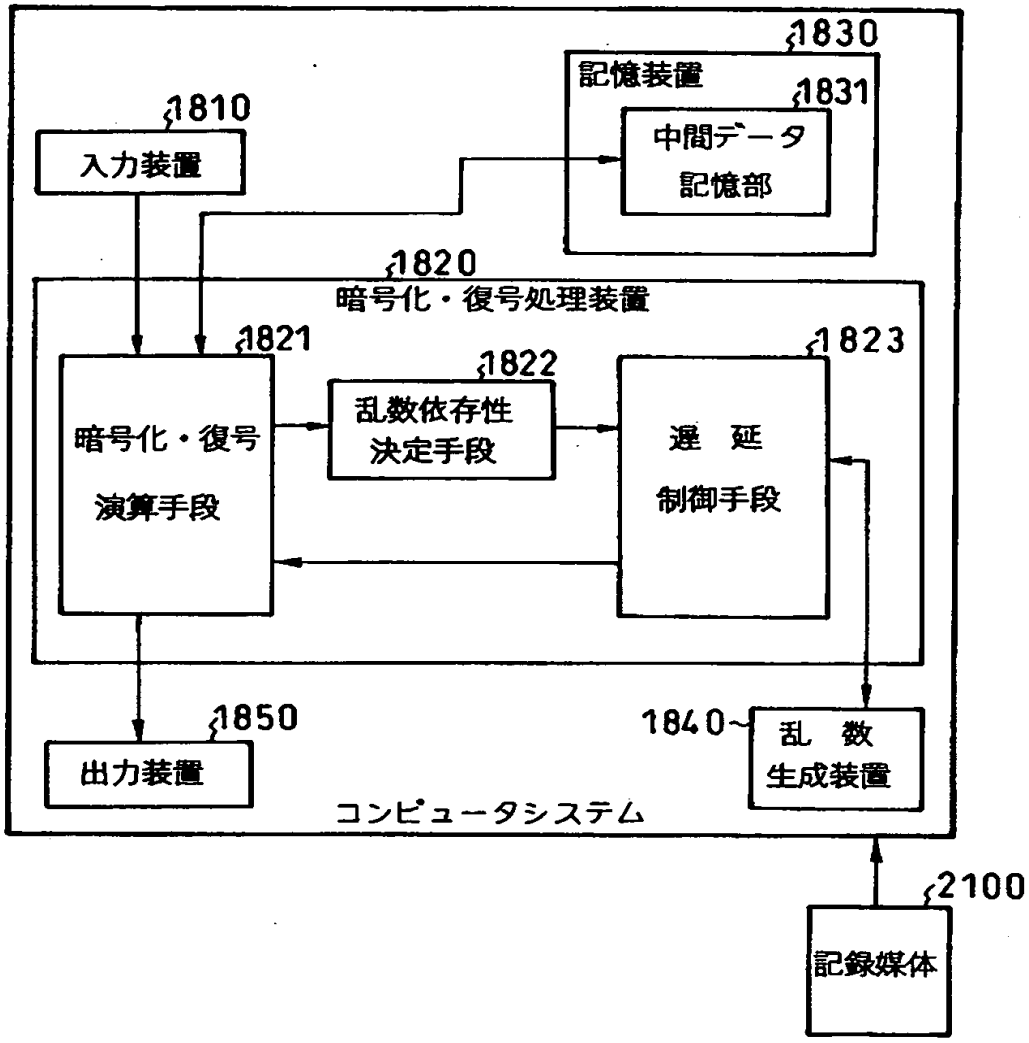
【図１９】


1630
記憶装置
1631
中間データ記憶部
1610
入力装置
1620
暗号化・復号処理装置
1621
暗号化・復号演算手段
1622
乱数依存性決定手段
1623
中間データ制御手段
1900
1650
出力装置
1640
乱　数生成装置
記録媒体
コンピュータシステム

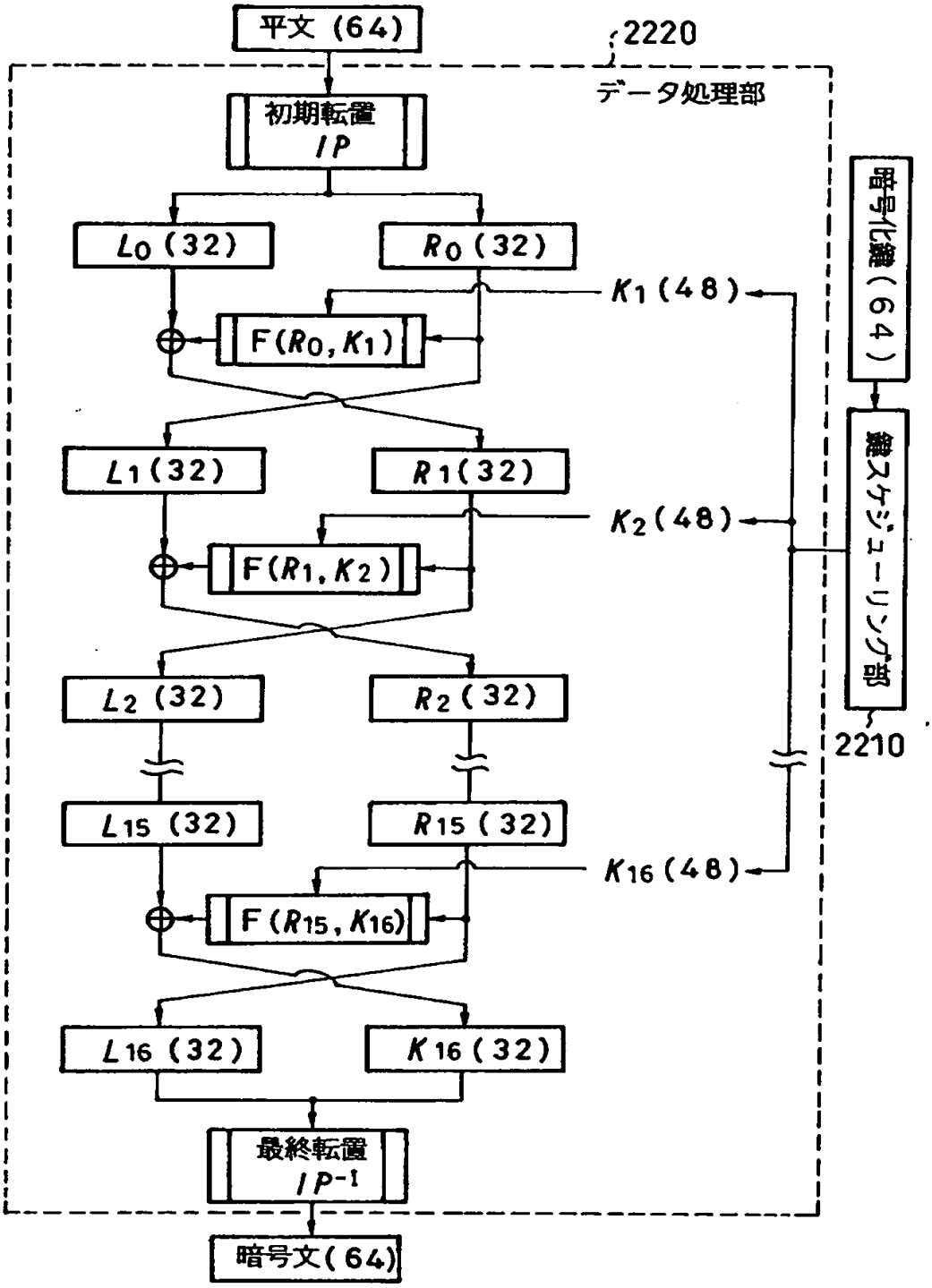
【図２０】


1730
記憶装置
1731
中間データ記憶部
1710
入力装置
1720
暗号化・復号処理装置
1721
暗号化・復号演算手段
1722
乱数依存性決定手段
1723
条件分岐制御手段
2000
1750
出力装置
1740
乱　数生成装置
記録媒体
コンピュータシステム

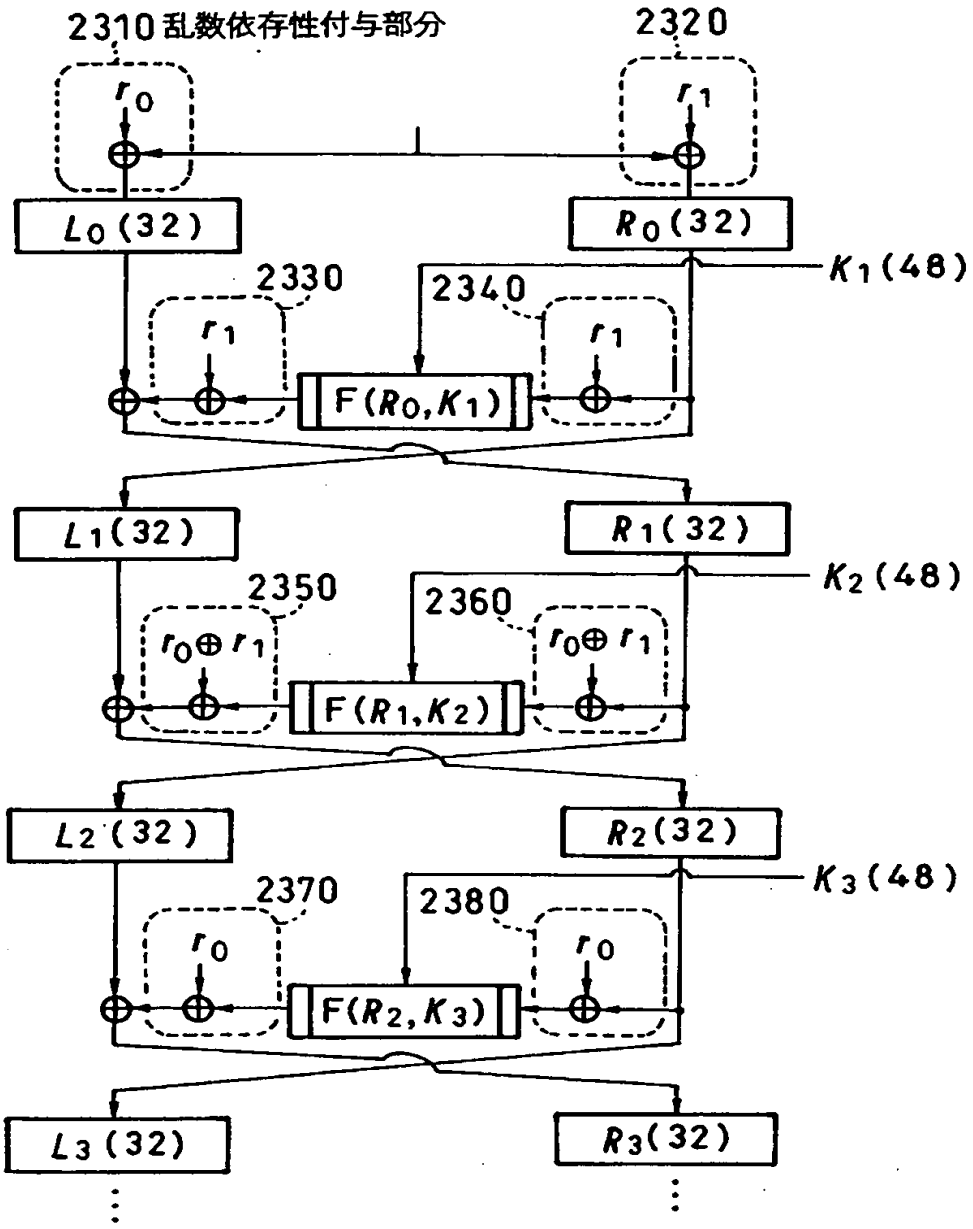
【図２１】


1830
記憶装置
1831
中間データ
記憶部
1810
入力装置
1820
暗号化・復号処理装置
1821
暗号化・復号
演算手段
1822
乱数依存性
決定手段
1823
遅　延
制御手段
1850
出力装置
1840
乱　数
生成装置
コンピュータシステム
2100
記録媒体

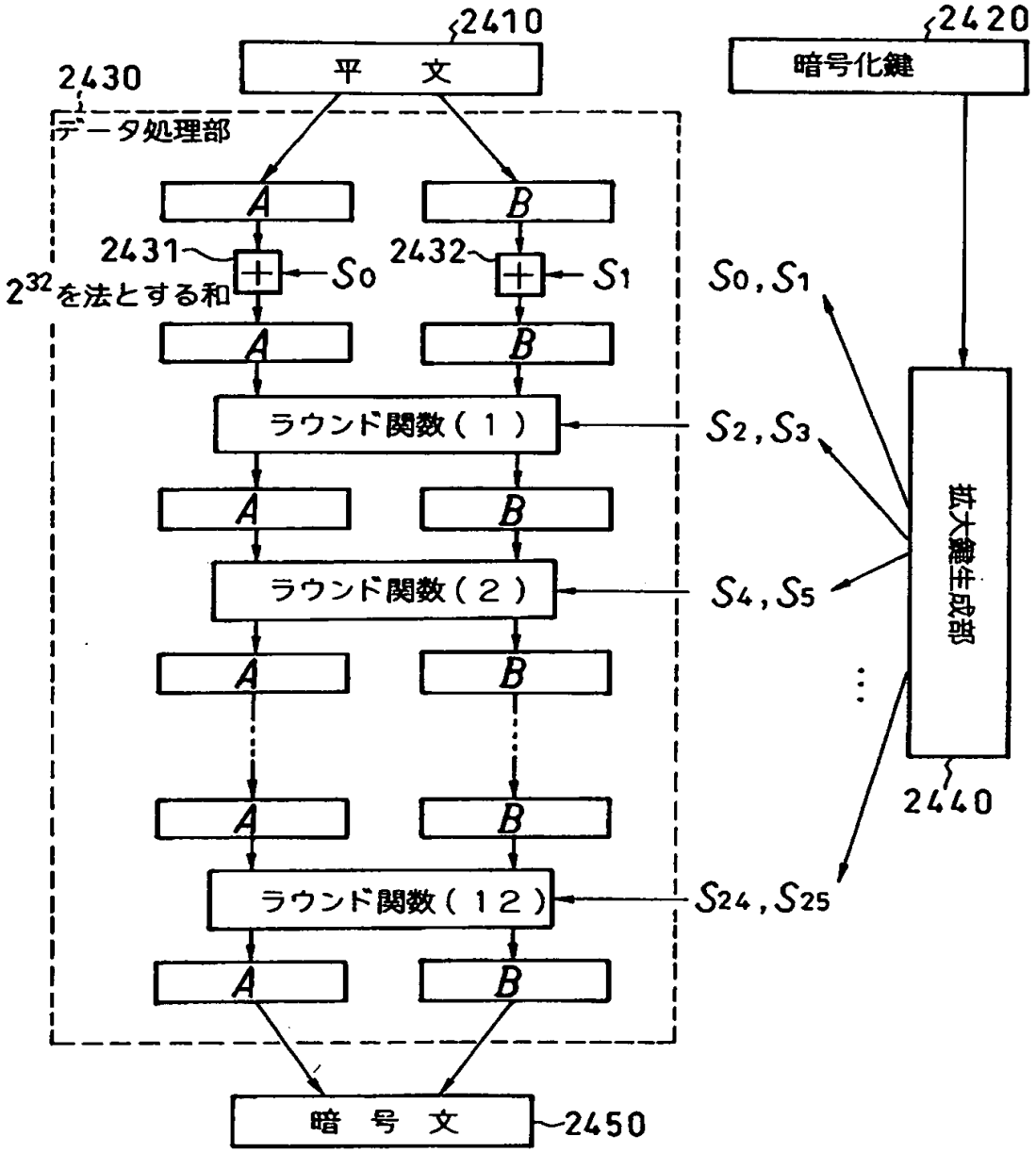
【図２２】


平文（64）
2220
データ処理部
初期転置
IP
L0（32）
R0（32）
K1（48）
F(R0, K1)
L1（32）
R1（32）
K2（48）
F(R1, K2)
L2（32）
R2（32）
L15（32）
R15（32）
K16（48）
F(R15, K16)
L16（32）
K16（32）
最終転置
IP-1
暗号文（64）
暗号化鍵（64）
鍵スケジューリング部
2210

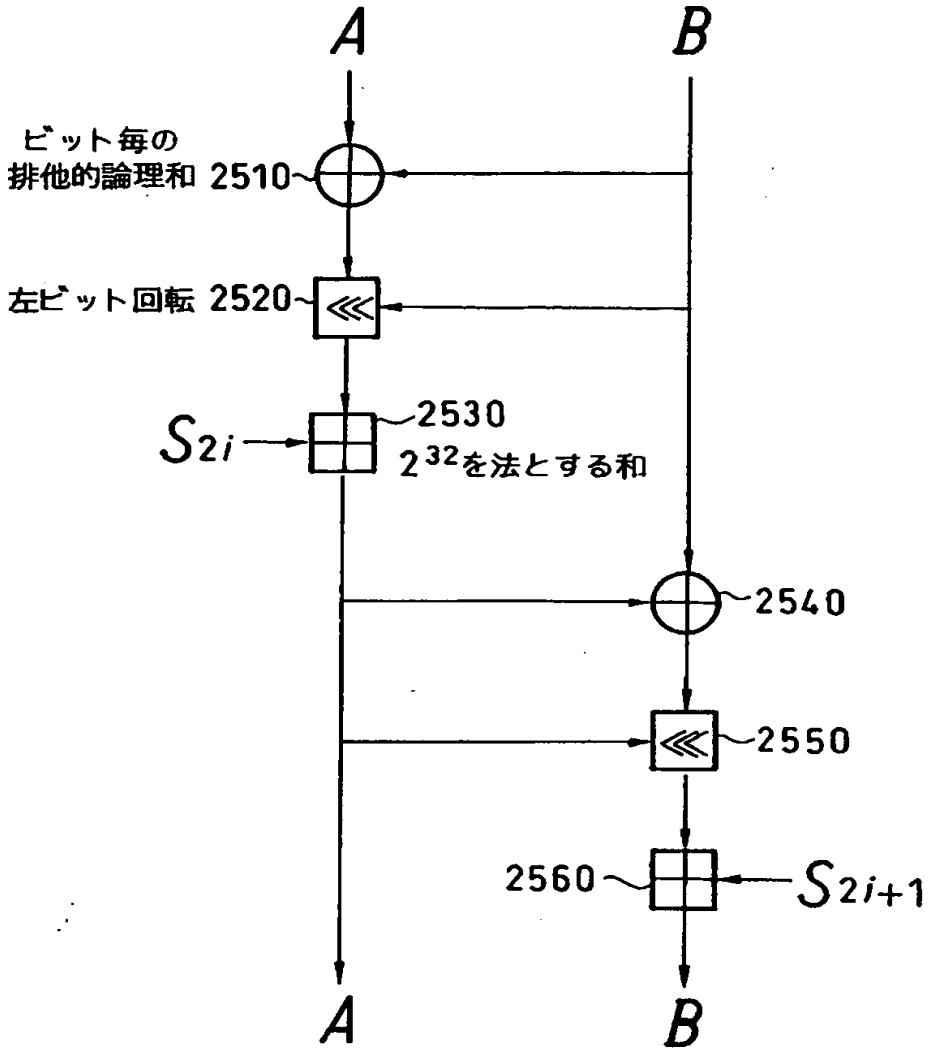
【図２３】


2310 乱数依存性付与部分
2320
r_0
r_1
$L_0(32)$
$R_0(32)$
$K_1(48)$
2330
2340
r_1
r_1
$F(R_0,K_1)$
$L_1(32)$
$R_1(32)$
$K_2(48)$
2350
2360
$r_0 \oplus r_1$
$r_0 \oplus r_1$
$F(R_1,K_2)$
$L_2(32)$
$R_2(32)$
$K_3(48)$
2370
2380
r_0
r_0
$F(R_2,K_3)$
$L_3(32)$
$R_3(32)$

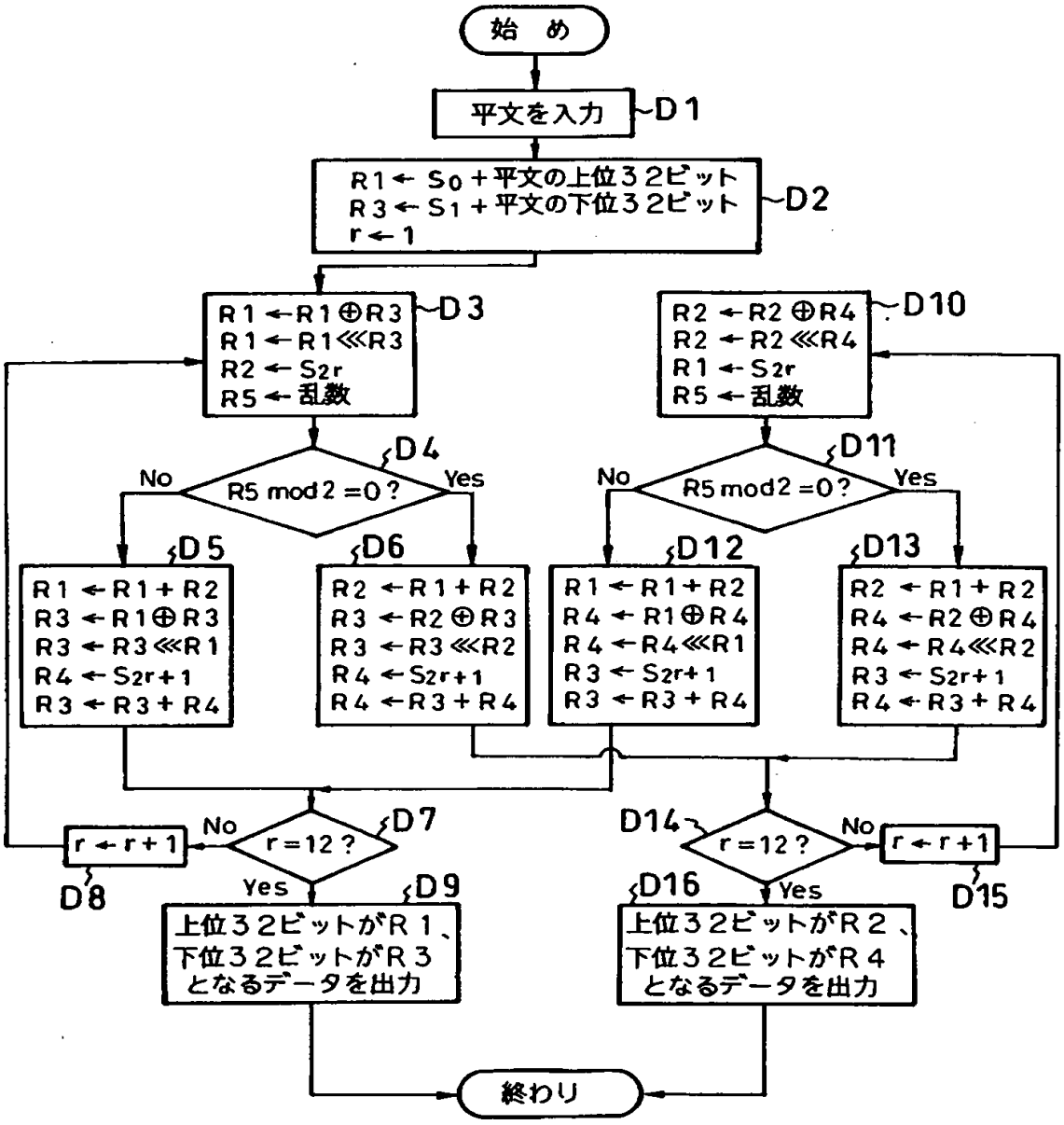
【図２４】


2410
平　文
2420
暗号化鍵
2430
データ処理部
A
B
2431
2432
2^{32}を法とする和
S0
S1
S0, S1
ラウンド関数（１）
S2, S3
ラウンド関数（２）
S4, S5
ラウンド関数（１２）
S24, S25
拡大鍵生成部
2440
暗　号　文
2450

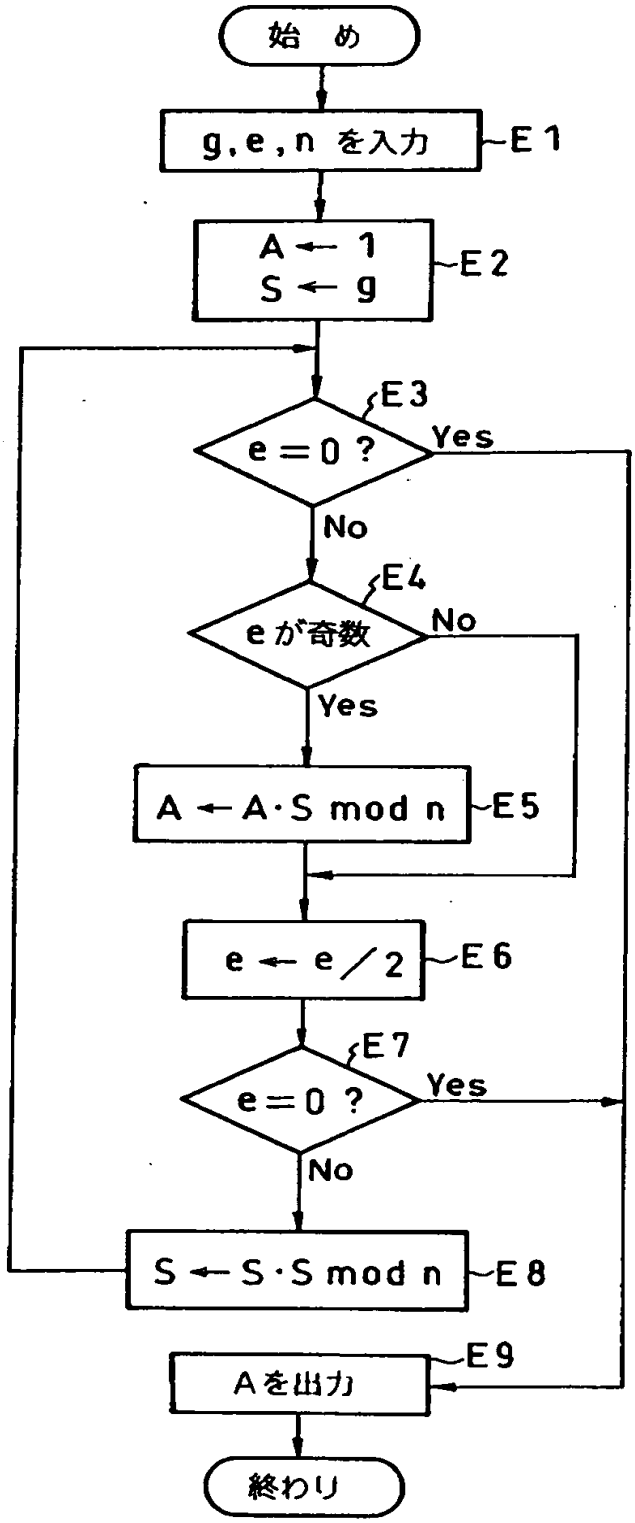
【図２５】


A
B
ビット毎の
排他的論理和 2510
左ビット回転 2520
S2i
2530
2^32を法とする和
2540
2550
2560
S2i+1
A
B

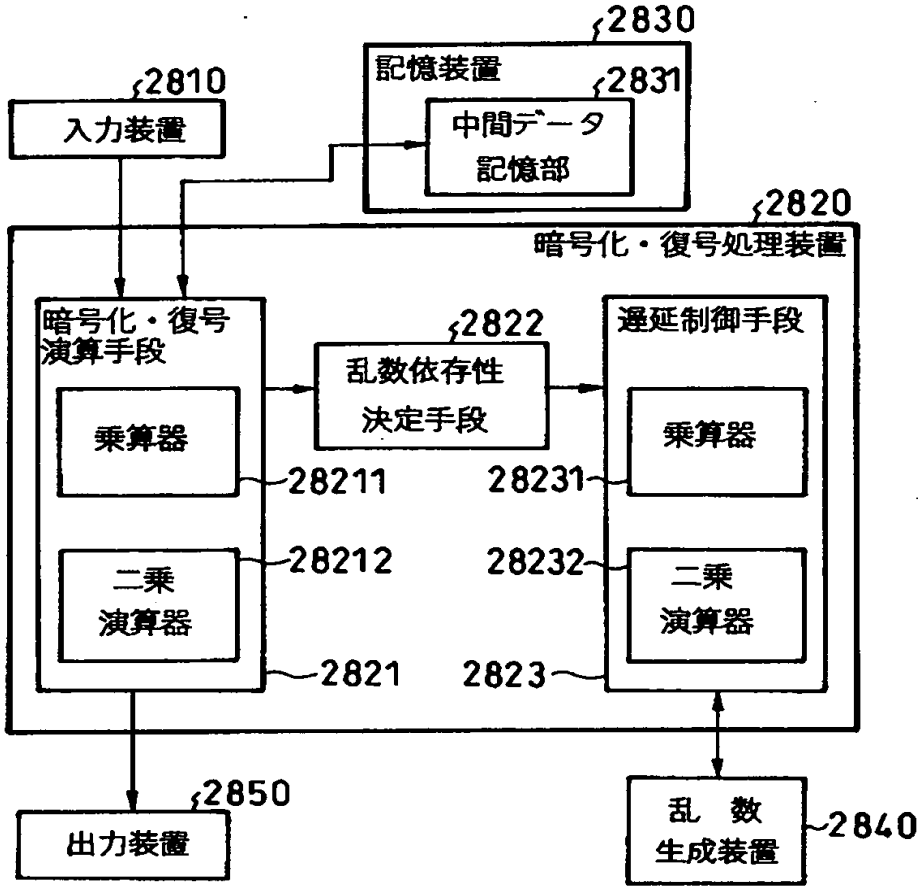
【図２６】


始　め
平文を入力
D1
R1 ← S0 + 平文の上位３２ビット
R3 ← S1 + 平文の下位３２ビット
r ← 1
D2
R1 ← R1 ⊕ R3
R1 ← R1 ≪ R3
R2 ← S2r
R5 ← 乱数
D3
R2 ← R2 ⊕ R4
R2 ← R2 ≪ R4
R1 ← S2r
R5 ← 乱数
D10
R5 mod 2 = 0 ?
No
Yes
D4
R5 mod 2 = 0 ?
No
Yes
D11
R1 ← R1 + R2
R3 ← R1 ⊕ R3
R3 ← R3 ≪ R1
R4 ← S2r+1
R3 ← R3 + R4
D5
R2 ← R1 + R2
R3 ← R2 ⊕ R3
R3 ← R3 ≪ R2
R4 ← S2r+1
R4 ← R3 + R4
D6
R1 ← R1 + R2
R4 ← R1 ⊕ R4
R4 ← R4 ≪ R1
R3 ← S2r+1
R3 ← R3 + R4
D12
R2 ← R1 + R2
R4 ← R2 ⊕ R4
R4 ← R4 ≪ R2
R3 ← S2r+1
R4 ← R3 + R4
D13
r ← r + 1
D8
No
r = 12 ?
Yes
D7
D9
上位３２ビットがＲ１、
下位３２ビットがＲ３
となるデータを出力
D14
r = 12 ?
No
Yes
r ← r + 1
D15
D16
上位３２ビットがＲ２、
下位３２ビットがＲ４
となるデータを出力
終わり

【図２７】


始　め
g,e,n を入力
E1
A ← 1
S ← g
E2
E3
e＝0？
Yes
No
E4
e が奇数
No
Yes
A ← A·S mod n
E5
e ← e／2
E6
E7
e＝0？
Yes
No
S ← S·S mod n
E8
E9
A を出力
終わり

【図２８】


2830
記憶装置
2831
中間データ記憶部
2810
入力装置
2820
暗号化・復号処理装置
暗号化・復号演算手段
乗算器
28211
二乗演算器
28212
2821
2822
乱数依存性決定手段
遅延制御手段
乗算器
28231
二乗演算器
28232
2823
2850
出力装置
乱数生成装置
2840

【書類名】　　要約書

【要約】

【課題】　電力解析や電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置，復号装置，および暗号化・復号装置を提供する。

【解決手段】　中間データ制御手段１２３は、乱数生成装置１４０から出力される乱数を入力として、中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する。暗号化演算手段１２１は、乱数依存中間データ変更操作に依存して状態を変化させつつ、平文に対する暗号化処理を実行し、乱数に依存しない暗号文を出力する。乱数依存性決定手段１２２は、暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、中間データ変更要求を発行する。

【選択図】　　図１

認定・付加情報

特許出願の番号	平成１１年　特許願　第１１４２３０号
受付番号	５９９００３８４６１５
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１１年　４月２３日

＜認定情報・付加情報＞

【提出日】　平成11年 4月21日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社